U.S. DEPARTMENT OF THE TREASURY

A Financial System That Creates Economic Opportunities

Nonbank Financials, Fintech, and Innovation

JULY 2018

U.S. DEPARTMENT OF THE TREASURY

A Financial System That Creates Economic Opportunities

Nonbank Financials, Fintech, and Innovation

Report to President Donald J. Trump

Executive Order 13772 on Core Principles
for Regulating the United States Financial System

Steven T. Mnuchin

Secretary

Craig S. Phillips

Counselor to the Secretary

Staff Acknowledgments

Secretary Mnuchin and Counselor Phillips would like to thank Treasury staff members for their contributions to this report. The staff's work on the report was led by Jessica Renier and W. Moses Kim, and included contributions from Chloe Cabot, Dan Dorman, Alexandra Friedman, Eric Froman, Dan Greenland, Gerry Hughes, Alexander Jackson, Danielle Johnson-Kutch, Ben Lachmann, Natalia Li, Daniel McCarty, John McGrail, Amyn Moolji, Brian Morgenstern, Daren Small-Moyers, Mark Nelson, Peter Nickoloff, Bimal Patel, Brian Peretti, Scott Rembrandt, Ed Roback, Ranya Rotolo, Jared Sawyer, Steven Seitz, Brian Smith, Mark Uyeda, Anne Wallwork, and Christopher Weaver.

Table of Contents

Acronyms and Abbreviations

Acronym/Abbreviation	Term
ABA	American Bankers Association
ACH	Automated Clearing House
AI	Artificial Intelligence
AMC	Appraisal Management Company
AML	Anti-Money Laundering
API	Application Programming Interface
APR	Annual Percentage Rate
AQB	Appraiser Qualifications Board
ASB	Appraisal Standards Board
ATM	Automated Teller Machine
AVM	Automated Valuation Model
BHC	Bank Holding Company
BHC Act	Bank Holding Company Act
BSA	Bank Secrecy Act
Bureau	Bureau of Consumer Financial Protection
CEG	Cybersecurity Expert Group
C.F.R.	Code of Federal Regulations
CFT	Countering the Financing of Terrorism
CFTC	U.S. Commodity Futures Trading Commission
CHAPS	Clearing House Automated Payment System
CHIPS	Clearing House Interbank Payments System
CMA	Competition and Markets Authority (U.K.)
CRA	Community Reinvestment Act
CROA	Credit Repair Organizations Act
CSBS	Conference of State Bank Supervisors
Cyber Apex	Next Generation Cyber Infrastructure Apex Program
DARPA	Defense Advanced Research Projects Agency
DHS	U.S. Department of Homeland Security
DIUx	Defense Innovation Unit Experimental

DLT	Distributed Ledger Technology
DOD	U.S. Department of Defense
Dodd-Frank	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	U.S. Department of Justice
DOL	U.S. Department of Labor
Education	U.S. Department of Education
EMV	Europay, Mastercard, and Visa
ESIGN	Electronic Signatures in Global and National Commerce Act
E.U.	European Union
FATF	Financial Action Task Force
FBIIC	Financial and Banking Information Infrastructure Committee
FCA	False Claims Act
FCA	U.K. Financial Conduct Authority
FCC	Federal Communications Commission
FCRA	Fair Credit Reporting Act
FDCPA	Fair Debt Collection Practices Act
FDIC	Federal Deposit Insurance Corporation
FedACH	Federal Reserve Banks' Automated Clearing House
FFIEC	Federal Financial Institutions Examination Council
FHA	Federal Housing Administration
FHA-HAMP	FHA Home Affordable Modification Program
FHFA	Federal Housing Finance Agency
FHLB	Federal Home Loan Bank
FICO	Fair Isaac Corporation
FIL	Financial Institutions Letter
FinCEN	Financial Crimes Enforcement Network
FINRA	Financial Industry Regulatory Authority
Fintech	Financial Technology
FIRREA	Financial Institutions Reform, Recovery, and Enforcement Act
FlexMod	GSE Flex Modification
FPS	Faster Payments Service (U.K.)

FRB	Board of Governors of the Federal Reserve System
FRBNY	Federal Reserve Bank of New York
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
FTC	Federal Trade Commission
G-7	Group of 7
G20	Group of 20
GAO	U.S. Government Accountability Office
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation (E.U.)
GLBA	Gramm-Leach-Bliley Act
GRC	Governance, Risk and Compliance
GSE	Government-Sponsored Enterprise
HUD	U.S. Department of Housing and Urban Development
IaaS	Infrastructure as a Service
IRS	Internal Revenue Service
ISO	International Organization for Standardization
IT	Information Technology
LOA	Levels of Assurance
MAS	Monetary Authority of Singapore
MBA	Mortgage Bankers Association
MBS	Mortgage-Backed Securities
MCSBA	Maryland Credit Services Business Act
MERS	Mortgage Electronic Registration System
MMIF	Mutual Mortgage Insurance Fund
MPL	Marketplace Lender
MSB	Money Services Business
MTRA	Money Transmitter Regulators Association
NACHA	National Automated Clearinghouse Association
NAIC	National Association of Insurance Commissioners
NBA	National Bank Act

NCUA	National Credit Union Administration
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NMLS	Nationwide Mortgage Licensing System or Nationwide Multistate Licensing System
NSF	National Science Foundation
NSS	National Settlement Service
OBIE	Open Banking Implementation Entity (U.K.)
OCC	Office of the Comptroller of the Currency
OFX	Open Financial Exchange
P2P	Person-to-Person or Peer-to-Peer
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PIN	Personal Identification Number
PLS	Private-Label Securities
PSD2	Revised Payment Services Directive (E.U.)
PSP	Payment Service Provider
RTP	Real Time Payments
SaaS	Software as a Service
SAFE Act	Secure and Fair Enforcement for Mortgage Licensing Act
SEC	U.S. Securities and Exchange Commission
SIFMA	Securities Industry and Financial Markets Association
SRO	Self-Regulatory Organization
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWIFT GPI	Society for Worldwide Interbank Financial Telecommunication Global Payments Innovation
TCH	The Clearing House
TCPA	Telephone Consumer Protection Act
TFFT	Basel Committee on Banking Supervision's Task Force on Financial Technology
Treasury	U.S. Department of the Treasury

U.K.	United Kingdom
U.S.	United States
UDAAP	Unfair, Deceptive, or Abusive Acts or Practices
UDAP	Unfair or Deceptive Acts or Practices
UETA	Uniform Electronic Transactions Act
URPERA	Uniform Real Property Electronic Recording Act
U.S.C.	United States Code
USDA	U.S. Department of Agriculture
USPAP	Uniform Standards of Professional Appraisal Practice
VA	U.S. Department of Veterans Affairs
ZB	Zettabyte

Executive Summary

Introduction

President Donald J. Trump established the policy of his Administration to regulate the U.S. financial system in a manner consistent with a set of Core Principles. These principles were set forth in Executive Order 13772 on February 3, 2017. The U.S. Department of the Treasury (Treasury), under the direction of Secretary Steven T. Mnuchin, prepared this report in response to that Executive Order. The reports issued pursuant to the Executive Order identify laws, treaties, regulations, guidance, reporting, and record keeping requirements, and other Government policies that promote or inhibit federal regulation of the U.S. financial system in a manner consistent with the Core Principles.

The Core Principles are:

A. Empower Americans to make independent financial decisions and informed choices in the marketplace, save for retirement, and build individual wealth;

B. Prevent taxpayer-funded bailouts;

C. Foster economic growth and vibrant financial markets through more rigorous regulatory impact analysis that addresses systemic risk and market failures, such as moral hazard and information asymmetry;

D. Enable American companies to be competitive with foreign firms in domestic and foreign markets;

E. Advance American interests in international financial regulatory negotiations and meetings;

F. Make regulation efficient, effective, and appropriately tailored; and

G. Restore public accountability within federal financial regulatory agencies and rationalize the federal financial regulatory framework.

Scope of This Report

The financial system encompasses a wide variety of institutions and services, and accordingly, Treasury has delivered a series of four reports related to the Executive Order covering:

- The depository system, covering banks, savings associations, and credit unions of all sizes, types, and regulatory charters (the Banking Report,[1] which was publicly released on June 12, 2017);
- Capital markets: debt, equity, commodities and derivatives markets, central clearing, and other operational functions (the Capital Markets Report,[2] which was publicly released on October 6, 2017);

1. U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Banks and Credit Unions* (June 2017).
2. U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Capital Markets* (Oct. 2017).

- The asset management and insurance industries, and retail and institutional investment products and vehicles (the Asset Management and Insurance Report,[3] which was publicly released on October 26, 2017); and
- Nonbank financial institutions, financial technology, and financial innovation (**this report**).

Review of the Process for This Report

For this report, Treasury incorporated insights from the engagement process for the previous three reports issued under the Executive Order and also engaged with additional stakeholders focused on data aggregation, nonbank credit lending and servicing, payments networks, financial technology, and innovation. Over the course of this outreach, Treasury consulted extensively with a wide range of stakeholders, including trade groups, financial services firms, federal and state regulators, consumer and other advocacy groups, academics, experts, investors, investment strategists, and others with relevant knowledge. Treasury also reviewed a wide range of data, research, and published material from both public and private sector sources.

Treasury incorporated the widest possible range of perspectives in evaluating approaches to regulation of the U.S. financial system according to the Core Principles. A list of organizations and individuals who provided input to Treasury in connection with the preparation of this report is set forth as ***Appendix A***.

Nonbank Financials, Fintech, and Innovation

Nonbank financial firms play important roles in providing financial services to U.S. consumers and businesses by providing credit to the economy across a wide range of retail and commercial asset classes. Nonbanks are well integrated into the U.S. payments system and play key roles such as facilitating back-end check processing; enabling card issuance, processing, and network activities; and providing customer-facing digital payments software. Nonbank financial firms also play important roles in capital markets and in providing financial advice and execution services to retail investors, among a range of other services.

The financial crisis altered the environment in which banks and nonbanks compete to provide financial services. Specifically, many traditional financial companies such as banks, credit unions, and insurance companies experienced significant distress during the crisis. This distress caused the insolvency or restructuring of many existing financial companies, particularly those with volatile funding sources and concentrated balance sheets. The government responded to this distress, and the unprecedented magnitude of taxpayer support it triggered, by writing far-reaching laws that mandated the adoption of hundreds of new regulations. In some cases, these policy changes made certain product segments unprofitable for banks, thereby driving activity

3. U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities: Asset Management and Insurance* (Oct. 2017).

outside of the banking sector and creating opportunities for emerging nonbank financial firms to address unmet market demands.

At the same time, and as part of a longer-term trend, the rapid development of financial technologies has enabled financial services firms to improve operational efficiencies and lower regulatory compliance costs that increased as a result of the expansion of regulations following the financial crisis. Since the financial crisis, there has been a proliferation in technological capabilities and processes at increasing levels of cost effectiveness and speed. The use of data, the speed of communication, the proliferation of mobile devices and applications, and the expansion of information flow all have broken down barriers to entry for a wide range of startups and other technology-based firms that are now competing or partnering with traditional providers in nearly every aspect of the financial services industry.

The landscape for financial services has changed substantially. From 2010 to the third quarter of 2017, more than 3,330 new technology-based firms serving the financial services industry have been founded, 40% of which are focused on banking and capital markets.[4] In the aggregate, the financing of such firms has been growing rapidly, reaching $22 billion globally in 2017, a thirteen-fold increase since 2010.[5] Significantly, lending by such firms now makes up more than 36% of all U.S. personal loans, up from less than 1% in 2010.[6] Additionally, some digital financial services reach up to some 80 million members,[7] while consumer data aggregators can serve more than 21 million customers.[8]

Important trends have arisen as a consequence of these factors, including:

- The nonbank sector has responded opportunistically to the pullback in services and increased regulatory challenges placed on traditional financial institutions, including the launch of numerous startup platforms;
- Many of these platforms have rapidly grown beyond the startup phase, employing technology-enabled approaches to customer acquisition and process support for their services;
- Innovative new platforms in the nonbank financial sector are, in some cases, standalone providers, while others have focused on providing support for or interconnectivity with traditional financial institutions through partnerships, joint ventures, or other means;

---

4. Deloitte, *Fintech by the Numbers: Incumbents, Startups, Investors Adapt to Maturing Ecosystem* (2017), at 3 and 7, available at: *https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-dcfs-fintech-by-the-numbers-web.pdf*.
5. Id.
6. Hannah Levitt, *Personal Loans Surge to a Record High*, Bloomberg (July 3, 2018), available at: *https://www.bloomberg.com/news/articles/2018-07-03/personal-loans-surge-to-a-record-as-fintech-firms-lead-the-way* (analyzing data from TransUnion).
7. Credit Karma, *Press Release – Credit Karma and Silver Lake Announce $500 Million Strategic Secondary Investment* (Mar. 28, 2018), available at: *https://www.creditkarma.com/pressreleases.*
8. Envestnet, *2017 Annual Report*, at 8, available at: *http://www.envestnet.com/report/2017/download/EN-2017-AnnualReport-Final.pdf*.

- Large technology companies with access to vast stores of consumer data have simultaneously entered the financial services industry, primarily in payments and credit provision; and
- The increasing scale of technology-enabled competitors and the corresponding threat of disruption has raised the stakes for existing firms to innovate more rapidly and pursue dynamic and adaptive strategies. As a result, mature firms have launched platforms aimed at reclaiming market share through alternative delivery systems and at lower costs than they were previously able to provide.

Consumers increasingly prefer fast, convenient, and efficient delivery of services. New technologies allow firms with limited scale to access computing power on levels comparable to much larger organizations. The relative ubiquity of online access in the United States, combined with these new technologies, allows newer firms to more easily expand their business operations.

In this report, we explore the characteristics of, and regulatory landscape for, nonbank financial firms with traditional "brick and mortar" footprints not covered in the previous Core Principles reports, as well as newer business models employed by technology-based firms. We also address the ability of banks to innovate internally, as well as partner with such technology-based firms. Foundational to the report's findings, we explore the implications of digitization and its impact on access to clients and their data, focusing on several thematic areas, including:

- The collection, storage, and use of financial data;
- Cloud services and "big data" analytics;
- Artificial intelligence and machine learning; and
- Digital legal identity and data security.

This report includes a limited treatment of blockchain and distributed ledger technologies. These technologies, as well as digital assets, are being explored separately in an interagency effort led by a working group of the Financial Stability Oversight Council. The working group is a convening mechanism to promote coordination among regulators as these technologies evolve.

Emerging Trends in Financial Intermediation

Financial services are being significantly reshaped by several important trends, including (1) rapid advances in technology; (2) increased efficiencies from the rapid digitization of the economy; and (3) the abundance of capital available to propel innovation.

Technological Advances in Financial Services

In addition to other benefits, innovations in financial technology expand access to services for underserved individuals or small businesses and improve the ease of use, speed, and cost of such services. Businesses providing financial services benefit from opportunities to improve their product offerings to win market share and reduce per-customer operational costs.

Expanded access to credit and financial services. Digital advice platforms are making financial planning tools and wealth management capabilities previously limited to higher net worth households available to a much broader segment of households. New platforms for lending are developing business models that take advantage of new types of data and credit analysis, potentially serving consumer and small business borrower segments that may not otherwise have access to credit through traditional underwriting approaches. Unbanked or underbanked populations can gain improved access to banking services through new mobile device-based banking applications.

Expanded speed, convenience, and security. Consumer and business demand for increased convenience and speed have driven the digitization of financial services. For example, increased digitization of the mortgage process has improved the online experience of financing a home, but additional innovations could dramatically help to further shorten the time it takes to close a mortgage, which still took an average of 52 days in 2016.[9] Borrowers seeking to refinance or consolidate higher-rate student loans or other consumer debts can obtain accelerated credit decisions from some lenders, as can small business entrepreneurs looking to expand their business or manage their seasonality.

Payment systems also benefit from innovations that are delivering greater speed and security. The proliferation of mobile and person-to-person payments allows end-users a way to quickly transfer money using identifiers such as an e-mail address or phone number. Contactless payment methods that store and tokenize payment information are also increasingly being used and could provide a more convenient and secure way to pay. These innovations are helping small businesses to lower the barriers to receive payments.

Reduced cost of services and operational efficiencies. Online marketplace lenders generally offer unsecured consumer loans that are designed to refinance existing higher-rate debts into lower-rate debt, reducing borrowing costs for consumers. Digital financial advice providers are able to leverage technology to scale their services to larger numbers of investors and to provide such services at more affordable prices than traditional providers. The increasing digitization of payments is expected to reduce significant costs in the current payment processes for businesses and firms by, for example, replacing physical paper checks with electronic payments and reducing inefficiencies in cross-border payments.

Digitization of Finance and the Economy

Changes in the hardware industry, as reflected in advances in core computing and data storage capacity, represent a sea change in capabilities and expand the potential for financial services to be provided on a more cost-effective basis. When considered alongside the ubiquity of mobile devices and the growth in the volume and facility of applications and flexibility of mobile communication, the implications for financial services are significant. The collection and storage of data and the application of advanced computational techniques allow for a new generation of approaches in the

9. Andreas Fuster et al., *The Role of Technology in Mortgage Lending*, Federal Reserve Bank of New York Staff Report No. 836 (Feb. 2018), at 12, available at: *https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr836.pdf*.

design, marketing, and delivery of financial services. At the same time, these new approaches may raise new concerns about data privacy and theft or misuse.

Consider the recent proliferation of digital data available for analysis. By 2020, digitized data is forecasted to be generated at a level that is more than 40 times the level produced in 2009.[10] In 2012, it was estimated that 90% of the digitized data in the world had been generated in just the prior two years.[11] Since 2012, more than one billion more people have gained access to the internet, with 2.5 billion people connected to the internet in 2012 and 3.7 billion people in 2017.[12] Globally, there are an estimated 27 billion devices connected to the internet, including smartphones, tablets, and computers, with expectations for 125 billion connected devices by the year 2030.[13]

Parallel to these growing improvements in data and connectivity are expanding complementary technologies, such as cloud computing and machine learning. These technologies enable firms to store vast amounts of data and efficiently increase computing resources. Unsurprisingly, for financial services firms, data analytics and machine learning (or artificial intelligence) are two of the top three areas of tech investment.[14] Other technology developments that are poised to impact innovation in financial services include advances in cryptography and distributed ledger technologies, giving rise to blockchain-based networks.

Investment Capital

The flow of capital into investments in financial technology is very large. U.S. firms accounted for nearly half of the $117 billion in cumulative global investments from 2010 to 2017.[15] Unfolding alongside these investments, many large, well-established firms involved in data, software, cloud computing, internet search, mobile devices, retail e-commerce, payments, and telecommunications have begun to engage in activities directly or indirectly related to financial services. Many of these firms are based in the United States, including firms having some of the largest market capitalizations in the world.

The availability of capital, the large size of the financial services market, and continued advancements in technology make accelerating innovation nearly inevitable. This includes investments in innovation by traditional financial institutions, such as banks, asset managers and insurers, to

---

10. A.T. Kearney, *Big Data and the Creative Destruction of Today's Business Models* (2013), at 2, available at: *https://www.atkearney.com/documents/10192/698536/Big+Data+and+the+Creative+Destruction+of+Today s+Business+Models.pdf/f05aed38-6c26-431d-8500-d75a2c384919* (discussing Oracle forecast).
11. Id.
12. Id.
13. IHS Markit, *The Internet of Things: A Movement, Not a Market* (Oct. 2017), at 2, available at: *https://cdn.ihs.com/www/pdf/IoT_ebook.pdf*. For projections that do not consider computers and phones, see Gartner, Inc., *Press Release – Gartner Says 8.4 Billion Connected "Things" Will be in Use in 2017, up 31 Percent from 2016* (Feb. 7, 2017), available at: *https://www.gartner.com/newsroom/id/3598917*.
14. PricewaterhouseCoopers, *Redrawing the Lines: FinTech's Growing Influence on Financial Services* (2017), at 9, available at: *https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintech-report-2017.pdf.*
15. Treasury analysis of FT Partners data.

provide higher quality, more secure, and more efficient services while meeting consumer demand for speed and convenience.

Summary of Issues and Recommendations

Treasury's review of the regulatory framework for nonbank financial institutions and innovation more broadly has identified significant opportunities to accelerate innovation in the United States consistent with the Core Principles. This review has identified a wide range of measures that could promote economic growth, while maintaining strong consumer and investor protections and safeguarding the financial system.

Treasury believes that innovation is critical to the success of the U.S. economy, particularly in the financial sector. Throughout Treasury's findings, opportunities have been identified to modernize regulation to embrace the use of data, encourage the adoption of advanced data processing and other techniques to improve business processes, and support the launch of alternative product and service delivery systems. Support of innovation is critical across the regulatory system — both at the federal and state levels. Treasury supports encouraging the launch of new business models as well as enabling traditional financial institutions, such as banks, asset managers, and insurance companies, to pursue innovative technologies to lower costs, improve customer outcomes, and improve access to credit and other services.

Treasury's recommendations in this report can be summarized in the following four categories:

- Adapting regulatory approaches to changes in the aggregation, sharing, and use of consumer financial data, and to support the development of key competitive technologies;
- Aligning the regulatory framework to combat unnecessary regulatory fragmentation, and account for new business models enabled by financial technologies;
- Updating activity-specific regulations across a range of products and services offered by nonbank financial institutions, many of which have become outdated in light of technological advances; and
- Advocating an approach to regulation that enables responsible experimentation in the financial sector, improves regulatory agility, and advances American interests abroad.

A list of all of Treasury's recommendations in this report is set forth as ***Appendix B***, including the recommended action, method of implementation (Congressional and/or regulatory action), and which Core Principles are addressed.

Key themes of Treasury's recommendations are as follows.

Embracing Digitization, Data, and Competitive Technologies

This report catalogues key elements in the evolution of digitization, data, and scalable technologies and highlights areas of relevance to many aspects of financial services, including lending, financial advice, and payments. Treasury recommends that key provisions of the Telephone Consumer

Protection Act be updated, and believes closing the digital divide to enable the entire U.S. population to benefit from modern information and communication flow is a priority.

Treasury makes numerous recommendations that would improve consumers' access to data and its use by third parties that would support better delivery of services in a responsible manner. Treasury has identified the need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data-sharing agreements that would effectively move firms away from screen-scraping to more secure and efficient methods of data access. The U.S. market would be well served by a solution developed in concert with the private sector that addresses data sharing, standardization, security, and liability issues. It is important to explore efforts to mitigate implementation costs for community banks and smaller financial services companies with more limited resources to invest in technology. Additionally, Treasury recommends that Congress enact a federal data security and breach notification law to protect consumer financial data and ensure that consumers are notified of breaches in a timely and consistent manner.

Removing regulatory barriers to foundational technologies, including the development of digital legal identity, is important to improving financial inclusion and enabling the use of scalable, competitive technologies. Similarly, facilitating the further development and incorporation of cloud technologies, machine learning, and artificial intelligence into financial services is important to realizing the potential these technologies can provide for financial services and the broader economy.

Aligning the Regulatory Framework to Promote Innovation

Many statutes and regulations addressing the financial sector date back decades. As a result, the financial regulatory framework is not always optimally suited to address new business models and products that continue to evolve in financial services. This has the potential negative consequence of limiting innovation that might benefit consumers and small businesses. Financial regulation should be modernized to more appropriately address the evolving characteristics of financial services of today and in the future.

It is important that state regulators strive to achieve greater harmonization, including considering drafting of model laws that could be uniformly adopted for financial services companies currently challenged by varying licensing requirements of each state. Treasury encourages efforts to streamline and coordinate examinations and to encourage, where possible, regulators to conduct joint examinations of individual firms. Treasury supports Vision 2020, an effort by the Conference of State Bank Supervisors that includes establishing a Fintech Industry Advisory Panel to help improve state regulation, harmonizing multi-state supervisory processes, and redesigning the successful Nationwide Multistate Licensing System.

At the federal level, Treasury encourages the Office of the Comptroller of the Currency to further develop its special purpose national bank charter, previously announced in December 2016. A forward-looking approach to federal charters could be effective in reducing regulatory fragmentation and growing markets by supporting beneficial business models.

Finally, Treasury encourages banking regulators to better tailor and clarify guidance regarding bank partnerships with nonbank financial firms, particularly smaller, less-mature companies with innovative technologies that do not present a material risk to the bank. Treasury believes it is important to encourage the partnership model to promote innovation. Further, Treasury makes recommendations regarding changes to permissible activities, including bank activities related to acquiring or investing in nonbank platforms.

Updating Activity-Specific Regulations

This report surveys a wide range of activities where specific recommendations for regulatory reform are suggested. The range of financial services includes:

Marketplace Lending

Marketplace lenders are expanding access to credit for consumers and businesses in the United States. Treasury recognizes that partnerships between banks and marketplace lenders have been valuable to enhance the capabilities of mature financial firms. Treasury recommends eliminating constraints brought about by recent court cases that would unnecessarily limit the functioning of U.S. credit markets. Congress should codify the "valid when made" doctrine and the role of the bank as the "true lender" of loans it makes. Federal banking regulators should also use their available authorities to address both of these challenges.

Mortgage Lending and Servicing

Treasury recognizes that the primary residential mortgage market has experienced a fundamental shift in composition since the financial crisis, as traditional deposit-based lender-servicers have ceded sizable market share to nonbank financial firms, with the latter now accounting for approximately half of new originations. Some of this shift has been driven by the post-crisis regulatory environment, including enforcement actions brought under the False Claims Act for violations related to government loan insurance programs. Additionally, many nonbank lenders have benefitted from early adoption of financial technology innovations that speed up and simplify loan application and approval at the front-end of the mortgage origination process. Policymakers should address regulatory challenges that discourage broad primary market participation and inhibit the adoption of technological developments with the potential to improve the customer experience, shorten origination timelines, facilitate efficient loss mitigation, and generally deliver a more reliable, lower cost mortgage product.

Student Lending and Servicing

The federal student loan program represents more than 90% of outstanding student loan volume and is managed by an extensive network of nonbanks for servicing and debt collection. The program is complex due to a variety of loan types, repayment plans, and product features that make the program difficult for borrowers to navigate and increase the difficulty and cost of servicing. Treasury recommends that the U.S. Department of Education establish and publish minimum effective servicing standards to provide servicers clear guidelines for servicing and help set expectations about how the servicing of federal loans is regulated. Treasury provides recommendations related to the greater use of technology in communications with borrowers, enhanced portfolio

performance monitoring and management by Education, and greater institutional accountability for schools participating in the federal financial aid programs.

Short-Term, Small-Dollar Lending

While the demand for short-term, small-dollar loans is high, lenders have been constrained by unnecessary regulatory guidance at the federal level. Treasury recommends that the Bureau of Consumer Financial Protection (Bureau) rescind its Payday Rule, which applies to nonbank short-term, small-dollar lenders, as the states already maintain the necessary regulatory authorities and the rule would further restrict consumer access to credit. Treasury also recommends that both federal and state banking regulators take steps to encourage prudent and sustainable short-term, small-dollar installment lending by banks.

Debt Collection

Debt collectors and debt buyers play an important role in minimizing losses in consumer credit markets, thereby allowing for increased availability of and lower priced credit to consumers. A variety of stakeholders have expressed concerns about the adequacy of loan information provided when a loan is sold or transferred for collection. When debt collectors and buyers do not receive adequate information, they are unable to demonstrate to the consumer that the debt is valid and owed. Treasury recommends the Bureau establish minimum effective federal standards for third-party debt collectors, including standards for the information that must be transferred with the debt for purposes of third-party collection or sale.

New Credit Models and Data

A growing number of firms have begun to use or explore a wide range of newer data sets or advanced algorithms, including machine learning-based methods, to support credit underwriting decisions. Treasury recognizes that these new credit models and data sources have the potential to meaningfully expand access to credit and the quality of financial services, and therefore recommends that financial regulators further enable their testing. In particular, regulators should provide regulatory clarity for the use of new data and modeling approaches that are generally recognized as providing predictive value consistent with applicable law for use in credit decisions.

Credit Bureaus

The consumer credit bureaus collect sensitive information on millions of Americans, and thus are required to protect the information they collect. While the credit bureaus are subject to state and federal regulation for consumer protection purposes, and have been subject to state and federal enforcement actions related to data security, they are not routinely supervised for compliance with the federal data security requirements of the Gramm-Leach-Bliley Act. Treasury recommends that the relevant agencies use appropriate authorities to coordinate regulatory actions to protect consumer data held by credit reporting agencies and that Congress continue to assess whether further authority is needed in this area. Treasury also recommends that Congress amend the Credit Repair Organizations Act to exclude national credit bureaus and national credit scorers in order to allow these entities to provide credit education and counseling services to consumers to prospectively improve their credit scores.

IRS Income Verification

The Internal Revenue Service (IRS) system that lenders and vendors use to obtain borrower tax transcripts is outdated and should be modernized in order to minimize delays in accessing tax information, which would facilitate the consumer and small business credit origination process. In other data aggregation situations, such as gathering borrower bank balances, lenders generally are able to obtain the needed borrower financial information through an application programming interface (API) to instantaneously and safely transfer data. The IRS's current technology should be updated to accommodate lender access of borrower information to instantaneously and safely transfer data, comparable to similar private sector solutions. While the IRS is working to update its technology more broadly, these efforts would benefit from additional funding, which would facilitate upgrades to support more efficient income verification, bringing a critical component of the credit process up to speed with broader innovations in financial technology.

Payments

Treasury recommends that the states work to harmonize money transmitter requirements for licensing and supervisory examinations, and urges the Bureau to provide more flexibility regarding the issuance of remittance disclosures. Treasury encourages the Federal Reserve to move quickly in facilitating a faster retail payments system, such as through the development of a real-time settlement service that would allow for more efficient and widespread access to innovative payment capabilities. Such a system should take into account the ability of smaller financial institutions, such as community banks and credit unions, to access innovative technologies and payment services.

Wealth Management and Digital Financial Planning

Digital financial planning tools can expand access to advice for Americans to accumulate sufficient wealth, particularly as individuals have become more responsible for their own retirement planning. Under the current regulatory structure, financial planners may be regulated at both the federal and state levels. Although many financial planners are regulated by the Securities and Exchange Commission or state securities regulators, they may also be subject to regulation by the Department of Labor, the Bureau, federal or state banking regulators, state insurance commissioners, state boards of accountancy, and state bars. This patchwork of regulatory authority increases costs and potentially presents unnecessary barriers to the development of digital financial planning services. Treasury recommends that an appropriate existing regulator of a financial planner be tasked with primary oversight of that financial planner and other regulators defer to that regulator.

Regulating a 21st Century Economy

Treasury advocates an agile approach to regulation that can evolve with innovation. It is critical not to allow fragmentation in the financial regulatory system, at both the federal and state level, to interfere with innovation. Financial regulators must consider new approaches to effectively promote innovation, including permitting meaningful experimentation by financial services firms to create innovative products, services, and processes.

Internationally, many countries have established "innovation facilitators" and various regulatory "sandboxes" — testing grounds for innovation. These sandboxes have each generally supported common principles, such as promoting the adoption and growth of innovation in financial services,

providing access to companies in various stages of the business lifecycle, providing varying degrees of regulatory relief while maintaining consumer protections, and improving the timeliness of regulator feedback offered throughout the development lifecycle. While replicating this approach in the United States is complicated by the fragmentation of our financial regulatory system, Treasury is committed to working with federal and state financial regulators to establish a unified solution that accomplishes these objectives — in essence, a regulatory sandbox.

The ability of regulators to engage with the private sector to test and understand new technologies and innovations as they arise is equally important. Treasury recommends that Congress pass legislation authorizing financial regulators to use other transaction authority for research and development and proof of concept technology projects. Treasury encourages financial regulators to pursue robust engagement efforts with industry and establish clear points of contact for outreach to enable the symbiotic relationship necessary to maintaining U.S. global competitiveness.

Treasury will work to ensure actions taken by international organizations align with U.S. national interests and the domestic priorities of U.S. regulatory authorities. This should include a focus on the needs of U.S. companies that operate on a global basis. Participation by the relevant experts in international forums and standard-setting bodies is important to share experiences regarding respective regulatory approaches and to benefit from lessons learned.

A Bright Future for Innovation

The United States is the global leader in technological innovation. The pace of technological development in financial services has increased exponentially, offering potential benefits to the U.S. economy. Treasury encourages all financial regulators to stay abreast of developments in technology and to properly tailor regulations in a manner that does not constrain innovation. Regulators must be more agile than in the past in order to fulfill their statutory responsibilities without creating unnecessary barriers to innovation. Ensuring a bright future for financial innovation, regulators should take meaningful steps to facilitate and enhance the nation's strength in technology and work toward the common goals of fostering vibrant financial markets and promoting growth through responsible innovation.

Embracing Digitization, Data, and Technology

Overview

The cost of collecting, transmitting, and storing vast amounts of data has sharply declined over the last 20 years, which has driven a technological revolution in many industries. Related technologies built on top of this increased ability to collect and manage data, like machine learning and artificial intelligence, have enabled a wide range of practical applications, many of which are relevant to the financial services industry. The combination of digitization, data, and technology can promote economic growth, increase consumer satisfaction, and improve choice, opportunity, and economic inclusion for all Americans. These factors also stimulate innovation, increase competition, and enhance the global competitiveness of the United States.

Key upgrades to the regulatory system are needed to enable the financial system to realize the benefits of economy-wide advances in these new technologies, including updating rules for financial services in the digital economy, assuring the existence of secure and open access to financial data, and aligning requirements for core infrastructure and competitive technologies. In each instance, there is a significant role for both the public and private sector — in fact, collaboration between the two is essential. Likewise, many regulations were adopted in and for a very different era, requiring a focus on modernization and appropriate tailoring that is consistent with the Core Principles.

Digitization

The transformation of business into the digital era has had a profound impact on innovation and economic growth. Converting information into digital form made it possible for data to be electronically stored, transmitted, and analyzed. As the costs of storing and processing data have decreased, the amounts of data collected and retained have correspondingly increased. When combined with developments in communication and networking, the modern economy exists in a digital environment that allows near-instantaneous access to significant volumes of information. Ensuring this data is used in a manner that safely creates new products and services with positive effects on the economy and society is an important national objective.

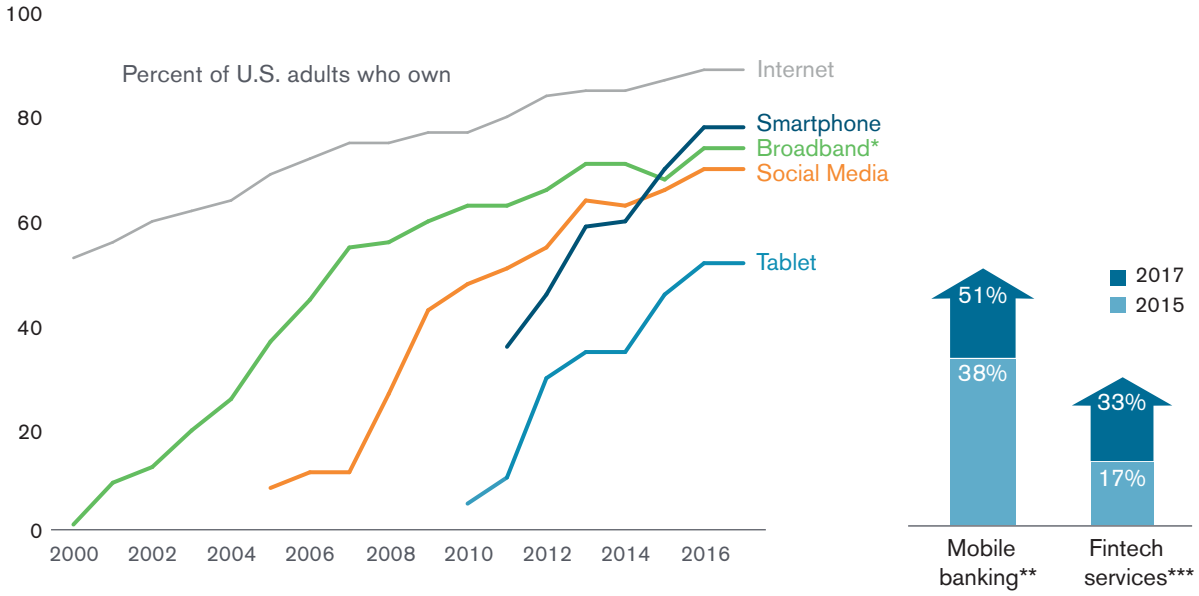
The key driver of this digital business environment is the increasingly widespread use of digital devices by Americans. Consider that nearly 90% of U.S. adults are online.[16] Moreover, 77% own a mobile phone with advanced digital capabilities, 53% own a tablet, and 46% have used digital voice assistants.[17] Most Americans use a combination of phone calls, text messages, and e-mails to manage their business and personal relationships. As a result, Americans' digital addresses (e.g., e-mail, device, chat ID) have increasingly become the equivalent of what a physical mailing address or telephone landline was in the past — the most effective way to reach a person for a business purpose.

---

16. Pew Research Center, *Internet/Broadband Fact Sheet* (Feb. 5, 2018), available at: *http://www.pewinternet.org/fact-sheet/internet-broadband/*.

17. Kenneth Olmstead, Pew Research Center, *Nearly Half of Americans Use Digital Voice Assistants, Mostly on their Smartphones* (Dec. 12, 2017), available at: *http://www.pewresearch.org/fact-tank/2017/12/12/nearly-half-of-americans-use-digital-voice-assistants-mostly-on-their-smartphones/*; Pew Research Center, *Mobile Fact Sheet* (Feb. 5, 2018), available at: *http://www.pewinternet.org/fact-sheet/mobile/*.

Figure 1: Technology Adoption and Usage



* used at home.
** as a percentage of survey respondents that have a bank account.
*** as a percentage of survey respondents that are active online.
Source (left): Chart and data recreated from Pew Research Center analysis.
Sources (right): For mobile banking data, Federal Reserve analysis of Survey of Household Economics and Decisionmaking and Survey of Consumers' Use of Mobile Financial Services.
For fintech services growth, see Ernst and Young, *EY FinTech Adoption Index 2017*, at 13.

Financial institutions and technology-focused firms have recognized this shift in where consumers "reside" and have consequently been transforming their business activities to meet customers' demand for digital interaction where possible. Consumers are rapidly adopting services provided by new fintech companies. Survey data indicate that up to one-third of online U.S. consumers use at least two fintech services — including financial planning, savings and investment, online borrowing, or some form of money transfer and payment.[18]

Banking is also increasingly digital. Today, 50% of people with bank accounts use mobile devices to access their information, up from 20% in 2011,[19] while the number of physical bank branches

18. Ernst & Young Global Limited, *EY FinTech Adoption Index 2017: The Rapid Emergency of FinTech* (2017), available at: *https://www.ey.com/Publication/vwLUAssets/ey-fintech-adoption-index-2017/%24FILE/ey-fintech-adoption-index-2017.pdf*.

19. Ellen A. Merry, Board of Governors of the Federal Reserve System, *Mobile Banking: A Closer Look at Survey Measures*, FEDS Notes (Mar. 27, 2018), available at: *https://doi.org/10.17016/2380-7172.2163*.

has been declining since 2009.[20] U.S. banks of all sizes are enabling digital engagement with their customers and are increasingly offering mobile phone applications that provide for a full suite of banking services, among other efforts.

This digital transformation of the economy and financial services requires wide-ranging changes to the U.S. regulatory system. For example, there is a need to modernize regulations for digitally communicating with consumers. Other regulations that should be implemented are discussed throughout this report and include: updating regulations to better facilitate secure access to digitized data, authentication of digital identity, and support for core financial service activities such as lending, payments, and investment advice.

Digital Communications

Telephone Consumer Protection Act

In 1991, Congress passed the Telephone Consumer Protection Act (TCPA) to restrict telemarketing calls and the use of automatic telephone dialing systems (autodialers) and prerecorded voice messages.[21] The Federal Communications Commission (FCC) is responsible for rules implementing the TCPA. Among the restrictions, the TCPA forbids telemarketers from calling a cell phone using an autodialer without first obtaining prior express consent of the called party.[22] However, current implementation of the TCPA constrains the ability of financial services firms to use digital communication channels to communicate with their customers despite consumers' increasing reliance on text messaging and e-mail communications through their mobile devices.

In 2015, the FCC issued an order responding to 21 requests for clarification or amendment to the FCC's TCPA rules and orders.[23] Financial services firms raised three primary concerns with the FCC's 2015 order. First, the definition of autodialer was overly broad because it included the capacity to make an autodialed call, as opposed to the actual use of the equipment as an autodialer. Second, by only providing a one-call safe harbor, which permitted a caller only a single call to determine whether a phone number was reassigned, the FCC order exposed firms to significant liability — up to a $500-per-call penalty — for dialing reassigned numbers, even when one call was insufficient to permit the firm to learn that the number was reassigned. Third, the order permitted consumers to revoke consent "using any reasonable method," and prohibited callers from "infring[ing] on that ability by designating an exclusive means to revoke."[24] Regarding revocation, firms asked for clear guidance detailing reasonable methods of revocation given the TCPA's penalties for noncompliance.

---

20. Julie Stackhouse, Federal Reserve Bank of St. Louis, *Why Are Banks Shuttering Branches?*, On the Economy Blog (Feb. 26, 2018), available at: *https://www.stlouisfed.org/on-the-economy/2018/february/why-banks-shuttering-branches*.
21. Public Law No. 102-243 [codified at 47 U.S.C. § 227].
22. 47 U.S.C. § 227(b)(1)(A).
23. See Federal Communications Commission, In the Matter Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al., *Declaratory Rule and Order*, CG Docket No. 02-278 (June 18, 2015), available at: *https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1_Rcd.pdf* ("FCC 2015 Order").
24. Id. at 7996.

On March 16, 2018, the U.S. Court of Appeals for the D.C. Circuit ruled on these three issues in a case brought against the FCC by ACA International, a trade group representing debt collectors.[25] First, the D.C. Circuit held that the FCC's definition of autodialer was arbitrary and capricious because, under the FCC's definition, "all smartphones qualify as autodialers because they have the inherent 'capacity' to gain [autodialer] functionality by downloading an app."[26] Second, the Court held that the one-call safe harbor was arbitrary and capricious because the FCC failed to explain why a "caller's reasonable reliance on a previous subscriber's consent necessarily cease[s] to be reasonable once there has been a single, post-reassignment call."[27] Third, the Court upheld the FCC's use of a "reasonable means" standard for revocation of consent but left open the possibility of different "revocation rules mutually adopted by contracting parties."[28]

After the D.C. Circuit's decision, the FCC reconsidered how the TCPA applies to reassigned numbers, issuing a proposed rule on preventing unwanted calls to reassigned numbers and seeking comment on methods to establish a reassigned numbers database.[29] A reassigned numbers database — long supported by market participants and consumer advocates — could reduce unwanted calls to consumers and reduce caller liability by permitting callers to conduct due diligence to learn whether a number has been recently reassigned and, if it has, remove that number from their autodialed calls.[30]

Fair Debt Collection Practices Act

Congress enacted the Fair Debt Collection Practices Act (FDCPA), in part, to "eliminate abusive debt collection practices by debt collectors."[31] The responsibility of enforcement is shared by the Bureau of Consumer Financial Protection (the Bureau) and the Federal Trade Commission (FTC).[32] However, current implementation of the FDCPA may inadvertently make interactions between debt collectors and consumers needlessly cumbersome. The FDCPA prohibits debt collectors from disclosing information about a consumer's debt to unauthorized third parties and allows consumers to terminate communication about the debt.[33] While using e-mail or voicemail to communicate with a consumer about his or her debt is permissible under FDCPA, potential litigation risk can arise if the debt collector inadvertently discloses information regarding the debt to an unauthorized third party while using contact information provided by the borrower. As a result, even if consumers increasingly prefer to communicate digitally, such as via text messages and e-mail, litigation risk can discourage debt collectors from doing so.

---

25. *ACA International v. FCC*, 885 F.3d 687 (D.C. Cir. 2018).
26. Id. at 700.
27. Id. at 707.
28. Id. at 709-10.
29. Advanced Methods to Target and Eliminate Unlawful Robocalls (Apr. 20, 2018) [83 Fed. Reg. 17631 (Apr. 23, 2018)].
30. Id.
31. 15 U.S.C. § 1692(e).
32. Id. § 1692*l*; see also Bureau of Consumer Financial Protection, *Fair Debt Collection Practices Act: Annual Report 2018* (Mar. 2018), at 7, available at: *https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_fdcpa_annual-report-congress_03-2018.pdf*.
33. 15 U.S.C. § 1692c(b).

Recommendations

Treasury recognizes that the increasingly digitized nature of the economy and financial system requires revisiting of customer communication and disclosure rules that were designed primarily for an era of physical mail and telephone calls. Treasury has identified some opportunities for reform of the TCPA and FDCPA regulatory regimes but recommends that regulators proactively identify other rules in need of revision.

Treasury recommends that the FCC continue its efforts to address the issue of unwanted calls through the creation of a reassigned numbers database. Treasury recommends that the FCC create a safe harbor for calls to reassigned numbers that provides callers a sufficient opportunity to learn that the number has been reassigned.

In addition, Treasury recommends that the FCC provide clear guidance on reasonable methods for consumers to revoke consent under the TCPA.

Additionally, Congress should consider statutory changes to the TCPA to mitigate unwanted calls to consumers and provide for a revocation standard similar to that provided under the FDCPA.

Treasury also recommends that the Bureau promulgate regulations under the FDCPA to codify that reasonable digital communications, especially when they reflect a consumer's preferred method, are appropriate for use in debt collection.

Closing the Digital Divide

"Digital divide" describes the gap between populations that have access to modern information and communication technology and those that have no or limited access. The FCC estimates 30% of people living in rural America lack access to broadband compared to 2.1% of people in urban areas, which means that nearly 24 million rural Americans cannot fully access the benefits of the digital economy.[34] Access to the digital economy allows Americans to benefit from the rapid growth of technology and innovation.

Broadband access has become increasingly important for economic opportunity, job creation, education, and civic engagement. Rural communities have made large gains in adopting technology, but substantial segments of rural America still lack the infrastructure needed for high-speed internet, and any access that rural areas have is often slower than that of non-rural areas.[35] In February 2017, the FCC took action designed to expand and preserve mobile coverage across rural America and in tribal lands.[36] The FCC stated that the next stages of the

34. Federal Communications Commission, *2018 Broadband Deployment Report* (Feb. 2, 2018), available at: *https://apps.fcc.gov/edocs_public/attachmatch/FCC-18-10A1.pdf*.

35. Andrew Perrin, Pew Research Center, *Digital Gap Between Rural and Nonrural America Persists*, blog post (May 19, 2017), available at: *http://www.pewresearch.org/fact-tank/2017/05/19/digital-gap-between-rural-and-nonrural-america-persists/*.

36. Federal Communications Commission, In the Matter of Connect America Fund Universal Service Reform – Mobility Fund, *Report and Order and Further Notice of Proposed Rulemaking* (Feb. 23, 2017), available at: *https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-11A1_Rcd.pdf*.

Connect America Fund[37] will be implemented and will provide additional funding for rural fixed broadband over the next decade.[38]

Additional support for these efforts is reflected in Executive Order 13821, which states that "it shall therefore be the policy of the executive branch to use all viable tools to accelerate the deployment and adoption of affordable, reliable, modern, high-speed broadband connectivity in rural America."[39] Concurrently, the President instructed the Secretary of the Interior to develop a plan to increase access to tower facilities and other infrastructure managed by the Department of the Interior in rural America for broadband deployment.[40]

Deployment of more infrastructure to support broadband in rural areas will help to close the digital divide and assist more Americans in underserved communities to participate in the digital economy and overcome geographic isolation.

Consumer Financial Data

As a result of digitization, vast amounts of data now exist in forms that can be readily aggregated and analyzed with computing power. Online and mobile applications that draw on these data make it possible for consumers to view banking and other financial account information, often held at different financial institutions, on a single platform, monitor the performance of their investments in real-time, compare financial and investment products, and even make payments or execute transactions. Applications can also assist with automatic savings, budget advice, credit decisions, and fraud and identity theft detection in real-time.[41]

In short, digitized record-keeping and these applications have exponentially improved a consumer's ability to make financial decisions. It has given rise to a new sector of nonbank financial institutions focused on products and services utilizing data aggregation, based on data obtained with the consumer's consent. The rise of such financial institutions presents questions regarding the way in which they operate and are currently regulated.

37. The Connect America Fund, also known as the Universal Service High-Cost Fund, is the FCC's program to expand voice and broadband services for areas where they are unavailable.

38. Federal Communications Commission, *Connect America Fund Phase II Auction Scheduled for July 24, 2018 - Notice and Filing Requirements and Other Procedures for Auction 903* (Feb. 1, 2018), available at: *https://apps.fcc.gov/edocs_public/attachmatch/FCC-18-6A1.pdf*.

39. Executive Order 13821, *Streamlining and Expediting Requests to Locate Broadband Facilities in Rural America* (Jan. 8, 2018) [83 Fed. Reg. 1507 (Jan. 11, 2018)].

40. Executive Office of the President, *Supporting Broadband Tower Facilities in Rural America on Federal Properties Managed by the Department of the Interior* (Jan. 8, 2018) [83 Fed. Reg. 1511 (Jan. 12, 2018)].

41. See Letter from the Center for Financial Services Innovation to the Bureau of Consumer Financial Protection, *CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records* (Feb. 21, 2017), available at: *https://www.regulations.gov/document?D=CFPB-2016-0048-0047*.

Data Aggregation

Data aggregation generally refers to any process in which information from one or more sources is compiled and standardized into a summary form.[42] Often data are aggregated for specific business or research purposes such as statistical analysis, performance tracking, or recordkeeping. As of the end of June 2018, five of the largest publicly-traded U.S. companies by market capitalization are integral drivers of the digital economy and use data aggregation for telecommunications, logistics, marketing, social media, and other purposes.[43]

How Data Aggregation Works

At the most basic level, data aggregation in the financial services sector necessarily involves consumers, financial services firms, data aggregators, and consumer financial technology (fintech) application providers. "Consumers" are the individuals who are users of financial services and the principal providers of the information collected by financial service companies. In the consumer financial services data aggregation framework, consumers decide which applications to use in order to access their data, give consent for that access, and provide necessary authentication (i.e., login) information.

"Financial services companies" or "financial services firms" include banks, mutual funds, insurance companies, broker-dealers, wealth management firms, and other financial institutions that provide traditional retail banking, depository, credit, brokerage, investment, and other account management services to consumers. These companies are the sources of consumer financial account and transaction data.

"Data aggregators" are the firms that access, aggregate, share, and store consumer financial account and transaction data they acquire through connections to financial services companies. Aggregators are intermediaries between the fintech applications that consumers use to access their data, on the one hand, and the sources of data at financial services companies on the other. An aggregator may be a generic provider of data to consumer fintech application providers and other third parties, or it may be part of a company providing branded and direct services to consumers.

Finally, "consumer fintech application providers" are the firms that access consumer financial account and transaction data, either from data aggregators or financial services companies, in order to provide value-added products and services to consumers. Consumers access these services through "fintech applications" — i.e., the websites or mobile apps — created by these firms. Consumer fintech application providers may also have direct links to financial services companies in order to, for example, provide direct services to a bank's customers, access payments systems, or facilitate credit origination.

Operationally, the key data aggregation processes involve acquiring, compiling, standardizing, and disseminating consumer financial data. Data aggregators may differ in the breadth and sophistication of the aggregation services they offer, and may specialize in different types of data or target a

42. See also Request for Information Regarding Consumer Access to Financial Records (Nov. 14, 2016) [81 Fed. Reg. 83806, 83808-09 (Nov. 22, 2016)] ("Data Aggregation RFI").

43. These companies are Apple, Amazon, Alphabet [Google], Microsoft, and Facebook, based on Treasury analysis of Bloomberg data.

Figure 2: Participants in the Consumer Financial Services Data Aggregation Framework

Participant	Description	Role
Consumers	• Individuals	• Choose which fintech applications serve needs • Accept terms and conditions • Give consent for data sharing • Provide login credentials or other information for authentication
Data aggregators	• Firms that aggregate consumer financial data to share with other third-parties, e.g. consumer fintech application providers • Firms that aggregate consumer financial data to provide branded and direct services to consumers	• Compile consumer financial account and transaction data obtained (1) through consumer-provided credentials (e.g., screen-scraping) and/or (2) through authorized connections with financial services companies (e.g., APIs) • Provide data to consumer fintech application providers and other third-parties • May develop own fintech applications • Often invisible to consumers
Consumer fintech application providers	• Third-party firms offering value-added financial products and services to consumers	• Create and market fintech applications for consumers • Frequently rely on data from aggregators to run applications • Applications enable consumers to monitor accounts, track budget and financial goals, pay bills, make peer-to-peer payments, take out loans, receive investment advice, etc.
Financial services companies	• Retail banks and other depository institutions • Retail broker-dealers • Mutual fund companies • Wealth management firms • Insurance companies • Other traditional financial institutions	• Provide traditional banking, investment, insurance and other financial services to consumers • Sources of consumer financial account and transaction data • Data may be accessed directly (e.g., APIs) or indirectly (e.g., screen-scraping)

Source: Treasury staff analysis.

specific developer base.[44] Some data aggregators may focus on aggregating financial account balances, transactions data, or credit card activity, for example, or they may primarily support consumer fintech application providers geared toward offering specific products (such as auto loans or mortgages) or services (such as peer-to-peer payments or budget tracking).

44. For an account of the evolution of data aggregation services, see Michael Kitces, *The Six Levels of Account Aggregation #FinTech and PFM Portals for Financial Advisors*, blog post (Oct. 9, 2017), available at: *https://www.kitces.com/blog/six-levels-account-aggregation-pfm-fintech-solutions-accounts-advice-automation/*.

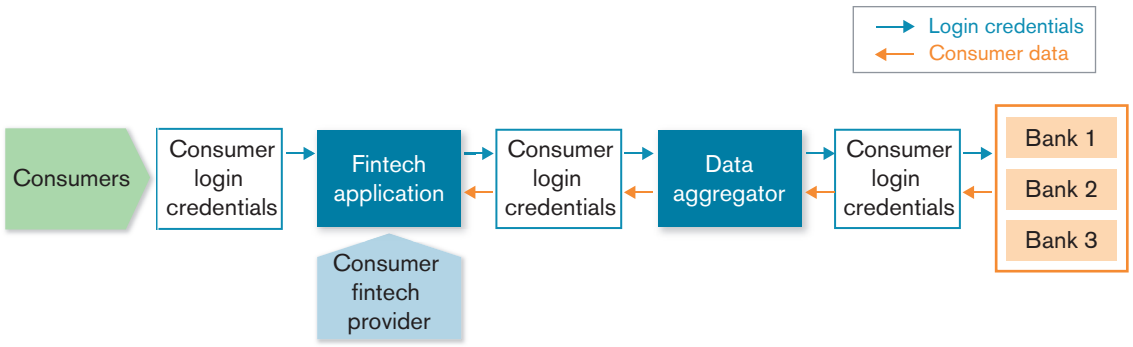
In general, data aggregators make data available by providing a platform on or through which consumer fintech application providers can build and run their applications and provide an interface with consumers. Because data aggregators are few in number compared to financial services companies — a relative handful versus thousands — and because they have generally sunk the costs of connecting to financial services companies, consumer fintech application providers only have to "build" to the data aggregators' specifications and not to hundreds or thousands of platforms run by individual financial institutions.[45]

Before these processes and interfaces can commence, however, a data aggregator requires access to consumers' data housed at financial services companies. At present, there are two primary methods through which data aggregators gain access to consumer financial data: "screen-scraping" and application programming interfaces (APIs).

Screen-Scraping

When data aggregators and consumer fintech application providers lack a direct connection to run fintech applications using data housed at financial services companies, they often rely on screen-scraping. In screen-scraping, consumers provide their account login credentials — usernames and passwords — in order to use the fintech application.[46] Consumers may or may not appreciate that they are providing their credentials to a third-party, and not logging in directly to their financial services company. Using these login credentials, data aggregators access consumers' financial

Figure 3: Screen-Scraping



Source: Treasury staff analysis.

45. By one data aggregator's account, there are eight major aggregators of consumer-authorized data in the United States. 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*. The listed data aggregators were Intuit, Quovo, Plaid, Envestnet/Yodlee, Morningstar/ByAllAccounts, Fiserv/CashEdge, Finicity, and MX.

46. Screen-scraping is not a recent development. As far back as 2001, regulators identified the practice of sharing consumer login credentials for data aggregation services as raising additional risks. See Office of the Comptroller of the Currency, *Bank-Provided Account Aggregation Services*, OCC Bulletin 2001-12 (Feb. 28. 2001), available at: *https://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-12.html*; Federal Financial Institutions Examination Council, *E-Banking*, IT Examination Handbook (Aug. 2003), at App. D, available at: *https://ithandbook.ffiec.gov/media/274777/ffiec_itbooklet_e-banking.pdf*.

accounts, and then, either manually or through specialized software, acquire the financial account and transaction data and even process data requests or execute transactions. Equally concerning, financial services companies are not always aware when screen-scraping methods are being used to access their customers' data.

Although screen-scraping can be an effective method of obtaining data, it is generally considered to have certain vulnerabilities and drawbacks. Many of the risks and concerns associated with data aggregation described in this report — whether for consumers, financial services companies, consumer fintech application providers, or data aggregators themselves — stem from the practice of screen-scraping.

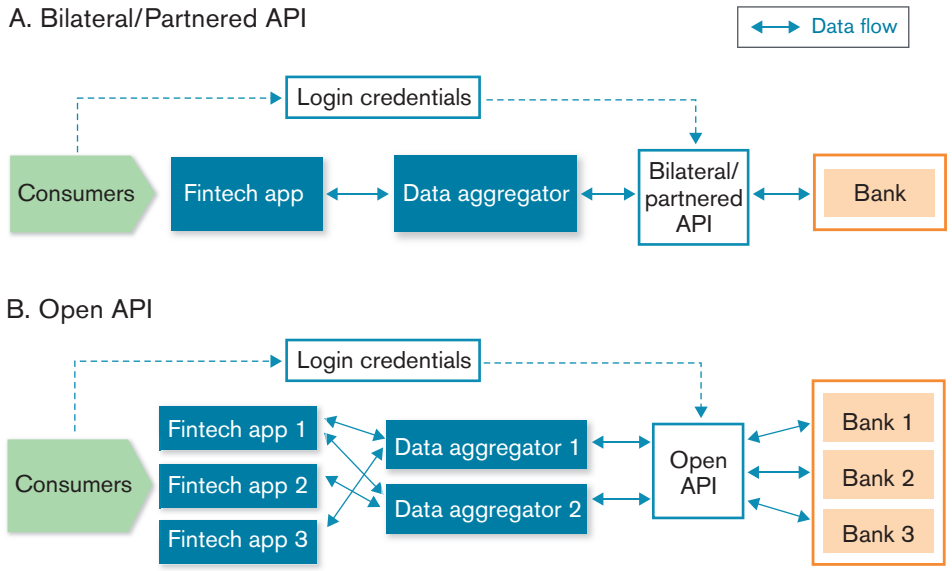
Application Programming Interfaces

The second method of accessing consumer financial account and transaction data is through an API or similar form of direct feed. For purposes of this report, an API can be loosely described as a clearly specified program that links two or more systems and that enables a well-defined communication and data exchange between them in order to run applications and other software. An API is not a specific technology, but rather a technology-enabled agreement or protocol that enables a computer system or source of data to interact with or be used by other software.[47] Unlike in the case of screen-scraping, data aggregation through an API generally means that financial services companies are knowingly participating in the sharing of data. As such, financial services companies can potentially deploy APIs that allow for the inclusion of robust security features, greater transparency and access controls for consumers, improved data accuracy, and more predictable and manageable information technology costs. APIs, however, cost money to develop, which could raise particular hurdles for smaller financial institutions with fewer information technology resources.

APIs may be designed to be open or they may be restricted to selected partners. In an open API, any third-party data aggregator or consumer fintech application provider that meets certain predetermined and published standards (e.g., security, licensing, etc.) can gain access to consumer data and build consumer-facing applications. In contrast, partnered APIs entail bilateral and exclusive agreements between financial services companies and data aggregators or consumer fintech application providers. In either case, the API method of access is generally enabled through consumer consent provided to the financial services company or at the API access point rather than through giving consumer login credentials to third-parties.

47. To illustrate how this works, think for example of nearly any app or website – for example, for ride-sharing services, retail stores, special events, etc. – that includes a map or the ability to provide point-to-point (or turn-by-turn) directions. These apps and websites generally do not create their own maps and navigation software. Instead, they would incorporate the maps and navigation software of an internet-based provider that specializes in aggregating mapping and navigation data. This provider makes its mapping and navigation products available for use by third-parties by establishing an API that includes instructions, tools, and other resources that enable software developers to incorporate such products into their own apps and websites.

Figure 4: Application Programming Interfaces (API)



Source: Treasury staff analysis.

Efforts to Improve Data Aggregation

Data aggregators, consumer fintech application providers, and financial services companies generally agree that consumers should have secure and reliable access to their financial account and transaction data, and that, in principle, consumers, if they opt-in, should be able to utilize fintech applications and other innovations that make use of their data. However, there is a lack of consensus on what secure and reliable access entails. As described by one observer, "the U.S. debate seems stuck at the yet-to-be resolved issue of migrating account aggregators from screen scraping-based to more secure and efficient API-based data-sharing methodologies."[48] As long as this impasse remains unresolved, consumers will be caught in the middle.

Consequently, data aggregators, consumer fintech application providers, and financial services companies in the United States are looking for better approaches to data aggregation. Despite the recognized advantages of using APIs as opposed to screen-scraping methods for data aggregation, current APIs have their limitations. Some data aggregators have entered into bilateral agreements to obtain data through an API, but this approach can be difficult to scale given the large number of U.S. financial services companies. In addition, data aggregators told Treasury that access through APIs was frequently and

48. Bob Hedges, The Clearing House, *Banking Perspectives: Consumer Data in an API-Enabled World* (4th Qtr. 2017), available at: *https://www.theclearinghouse.org/banking-perspectives/2017/2017-q4-banking-perspectives/articles/open-banking.*

unilaterally restricted, interrupted, or terminated by financial services companies.[49] Hence, Treasury's understanding is that a significant amount of data is still obtained through screen-scraping.

Much of the focus is on improving API methods to resolve issues such as standardizing data elements and fair and proportional allocation of liability and accountability in the event of a data breach. In some cases, participants from across the data aggregation framework are collaborating to develop robust open APIs that serve the needs of all stakeholders.[50] Further, trade groups are also starting to solidify views and have developed principles with respect to data aggregation.[51]

Open Banking in the United Kingdom

In considering regulatory approaches for data aggregation, the efforts in other countries that have created their own regulatory regimes for consumer access to financial account and transaction data can provide a useful comparison point. In August 2016, the United Kingdom's Competition and Markets Authority (CMA) issued a report, which concluded that the market for retail banking was not sufficiently competitive and was dominated by large banks. The CMA outlined a package of remedies called Open Banking, which required the nine largest U.K. banks to adopt "open API banking standards… [and] to make data available using these standards."[52] Other banks can opt-in on a voluntary basis.

---

49. See also Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals*, The Wall Street Journal (Nov. 4, 2015).

50. One such effort is being carried out through the OFX Consortium, the origins of which date back to 1997. The OFX specification is one of original standards for the exchange of financial information between consumers and financial services providers. In April 2016, the OFX Consortium released OFX 2.2, which introduced new standards including data tags and tokenized authentication solutions for sharing consumer financial data. See OFX Consortium, *OFX 2.2 Released with OAuth-Token based Authentication*, Business Wire (Apr. 7, 2016), available at: *https://www.businesswire.com/news/home/20160407006078/en/OFX-2.2-Released-OAuth-Token-based-Authentication*. A more recent effort is that of the Aggregation Services Working Group of the FS-ISAC. The Working Group, which consists of representatives from financial services companies, data aggregators, and fintech developers, recently issued the second version of its API for secure, tokenized data transfer. See Financial Services Information Sharing and Analysis Center, *Press Release – FS-ISAC Enables Safer Financial Data Sharing with API* (Feb. 13, 2018), available at: *https://www.fsisac.com/article/fs-isac-enables-safer-financial-data-sharing-api*.

51. See, e.g., Securities Industry and Financial Markets Association, *SIFMA Data Aggregation Principles* (Apr. 2018), available at: *https://www.sifma.org/wp-content/uploads/2018/04/sifma-Data-Aggregation-Principles.pdf*. The SIFMA principles affirm that consumers "may use third-parties to access their financial account data" and "such access should be safe and secure." See also Renee Hobbs, Envestnet|Yodlee, *Envestnet|Yodlee, Quovo and Morningstar ByAllAccounts: Statement of Joint Principles for Ensuring Consumer Access to Financial Data*, blog post (May 11, 2018), available at: *https://www.yodlee.com/blog/envestnet-yodlee-quovo-and-morningstar-byallaccounts-statement-of-joint-principles-for-ensuring-consumer-access-to-financial-data/*. These three data aggregators proposed a "Secure Open Data Access" framework, which includes the following four components: (1) consumers must be able to access their financial account data for purposes of using any legitimate application; (2) consumers must provide affirmative consent on the basis of clear and conspicuous disclosure regarding the use of their data; (3) all entities who handle consumer account information must adhere to best practices for security standards and implement traceability/transparency; and (4) the entity responsible for a consumer's financial loss must make the consumer whole.

52. See Competition and Markets Authority, *Retail Banking Market Investigation: Final Report* (Aug. 9, 2016), at 441-461, available at: *https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf*.

These remedies are aimed at increasing competition, including lowering costs for consumers switching between financial institutions.

The first stage of Open Banking went live in March 2017, when the covered banks were required to make certain "open data" — i.e., public information such as the location of branches and automated teller machines as well as the terms of certain banking products — widely available online. The full Open Banking standard came into effect in January 2018. The CMA established the nonprofit Open Banking Implementation Entity (OBIE) to work with banks and third-party fintech developers to help integrate with Open Banking and to test their products and services based on the data. Fintech developers enrolled in Open Banking must be regulated by the U.K. Financial Conduct Authority.[53]

Open Banking uses "read/write" APIs with standards and specifications defined by OBIE. To securely access and share data, the participating banks develop API "endpoints" on which fintech developers can build applications. The use of APIs permits consumers to retain full control over their account information. Consumers must give explicit consent before using any fintech applications and are redirected to their bank's login screen to enter their login credentials. Consumers determine which information can be accessed, for how long and for what purpose, and can revoke their consent at any time. Shared data is encrypted and its usage is tracked, and only regulated persons can access it.

There are significant differences between the United States and the United Kingdom with respect to the size, nature, and diversity of the financial services sector and regulatory mandates. Given those differences, an equivalent Open Banking regime for the U.S. market is not readily applicable. Nonetheless, as Open Banking matures in the United Kingdom, U.S. financial regulators should observe developments and learn from the British experience.

Issues and Recommendations

Consumers' ability to realize the benefits of data aggregation is limited, in part due to the lack of agreement between data aggregators and financial services companies over access to consumer financial account and transaction data. However, Treasury recognizes that significant strides have been made in recent years to bridge these disagreements. As information and data technology advances, and with sustained commitment to the principle that consumers should be able to freely access and use their financial account and transaction data, Treasury believes that improved approaches to data aggregation that will benefit consumers and financial institutions alike are surely attainable.

Consumer Access to Financial Account and Transaction Data

The only express statutory provision regarding access to a consumer's own financial account and transaction data is Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank).[54] It states that, subject to rules prescribed by the Bureau, financial services

53. As of July 2018, there were 33 regulated third-party providers enrolled in Open Banking. See *https://www.openbanking.org.uk/regulated-providers/*.

54. Codified at 12 U.S.C. § 5533.

companies subject to the Bureau's jurisdiction as covered persons[55] are required to make available to a consumer, upon request, certain financial account and transaction data concerning any product or service obtained by the consumer from that financial services company.[56] This data must be made available in an electronic form usable by the consumer.[57]

In November 2016, the Bureau issued a request for information to better understand the benefits and risks associated with market developments that rely upon data aggregation.[58] Subsequently, the Bureau published nonbinding principles in October 2017 expressing a vision for a "robust, safe, and workable data aggregation market,"[59] although it noted that "few, if any, individual stakeholders" enumerated all of the consumer protection concerns presented in the principles.[60]

As described by the Bureau, financial data subject to consumer and consumer-authorized access may include any transaction, series of transactions, or other aspect of consumer usage, the terms of any account, such as a fee schedule, realized consumer costs, such as fees or interest paid, and realized consumer benefits, such as interest earned or rewards.[61] The principles underscore the role of companies that access consumers' financial data, with their permission, in order to provide services that hold the promise of "improved and innovative consumer financial products and services."[62]

In addition to the Bureau, other groups have developed their own principles for data aggregation, including the Securities Industry and Financial Markets Association, the Consumer Financial Data Rights Coalition, and the Center for Financial Services Innovation.[63] While Treasury is not endorsing any particular set of principles, they contain common themes on topics such as security, access, and consumer consent, which can form the basis for consensus on consumer-authorized data aggregation.

---

55. Under Section 1002(6) of Dodd-Frank [12 U.S.C. § 5481(6)], a "covered person" is defined as "any person that engages in offering or providing a consumer financial product or service," and any affiliate of such a person, if the affiliate acts as a service provider to that person. Notwithstanding the broad definition of "covered person," other provisions place limits on the Bureau's jurisdiction for certain entities. See, e.g., 12 U.S.C. § 5517.

56. 12 U.S.C. § 5533(a). Section 1033, however, applies only to information that the covered person can retrieve in the ordinary course of its business with respect to that information. 12 U.S.C. § 5533(b)(4).

57. 12 U.S.C. § 5533(a).

58. Data Aggregation RFI.

59. Bureau of Consumer Financial Protection, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18, 2017), available at: *https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf* ("Bureau Data Principles").

60. Bureau of Consumer Financial Protection, *Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights that Inform the Consumer Protection Principles* (Oct. 18, 2017), at 2, available at: *https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf* ("Bureau Stakeholder Insights").

61. Bureau Data Principles, at 3.

62. Id. at 1.

63. See footnote 51. See also Center for Financial Services Innovation, *CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration* (Oct. 2016), available at: *https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2016/10/27001530/2016-Consumer-Data-Sharing-CDAWG-One-pager-Final-1.pdf*.

Direct Consumer Access Versus Consumer-Authorized Access

In response to the Bureau's request for information, conflicting views were expressed on whether data aggregators are covered by Section 1033.[64] Some financial services companies argued that access rights apply only to direct consumer access to their data but not to consumer-authorized access through a data aggregator or a fintech application. In contrast, consumer groups, data aggregators, and consumer fintech application providers asserted that consumers are entitled to access their financial account and transaction data via fintech applications.

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."[65] This definition is best interpreted to cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties such as data aggregators and consumer fintech application providers to access their financial account and transaction data from financial services companies. Otherwise, narrowly interpreting Section 1033 as applying only to direct consumer access would do little to advance consumer interests by eliminating many of the benefits they derive from data aggregation and the innovations that flow through from fintech applications.

Recommendation

Treasury recommends that the Bureau affirm that for purposes of Section 1033, third parties properly authorized by consumers, including data aggregators and consumer fintech application providers, fall within the definition of "consumer" under Section 1002(4) of Dodd-Frank for the purpose of obtaining access to financial account and transaction data.

Entities Covered by Data Access Requirements

Section 1033 applies only to "covered persons" under Dodd-Frank, which includes a subset of financial services companies. Furthermore, the Bureau's jurisdiction is subject to limitations for some financial services companies subject to regulation by other federal or state regulators, including: persons regulated by a state securities commission, to the extent that such persons act in a regulated capacity, or by the Securities and Exchange Commission (SEC);[66] persons regulated by the Department of Labor (DOL) that are offering 401(k) plans or employee benefit plans;[67] and persons regulated by state insurance regulators that are offering insurance products.[68]

Financial services companies primarily regulated by regulators other than the Bureau play important roles in the retirement savings plans of many Americans. While one approach is to expand the scope of Section 1033 to expressly include these companies, Treasury does not believe that step is necessary. Treasury has not identified evidence of market failure with respect to electronic access to data held by financial services companies not subject to Section 1033. In outreach meetings, financial planners and investment advisers advised Treasury that many broker-dealers and their

64. See Bureau Stakeholder Insights, at 4-5.
65. 12 U.S.C. § 5481(4).
66. See 12 U.S.C. § 5517(h)-(i).
67. See 12 U.S.C. § 5517(g).
68. See 12 U.S.C. § 5517(f).

custodians have been providing financial account and transaction data in a usable electronic format for a long time.[69] Such data, for instance, is needed to produce performance reports and monitor asset allocations. However, in outreach meetings with Treasury, financial planners and investment advisers indicated that the current data feeds from broker-dealers were generally reliable.

Recommendations

Treasury recommends that regulators such as the SEC, Financial Industry Regulatory Authority, DOL, and state insurance regulators recognize the benefits of consumer access to financial account and transaction data in electronic form and consider what measures, if any, may be needed to facilitate such access for entities under their jurisdiction.[70] However, Treasury recommends against further legislative action to expand the scope of Section 1033 at this time.

Consumer Disclosure, Consent, and Termination

The products and services discussed in this section require consumer authorization as the legal basis for accessing the financial account and transaction data. But consumers cannot make informed choices without transparent, comprehensible, and readily accessible disclosure. Without adequate disclosure, consumers will be unable to clearly understand and weigh the risks and benefits of using fintech applications and letting third-parties access and use their personal and financial data.

Some fintech applications and data aggregators make hard-to-follow disclosures as to which financial account and transaction data will be obtained and how that data will be utilized and stored. In other cases, the disclosures, terms, and conditions may be hard to find or they may be written in dense legalistic language that induces the consumer to head straight to the "accept" button, or else forgo usage of the service.

Disclosures may not be fully effective to the extent that consumers remain unaware of the data relationships underlying the services they are using. For example, for fintech applications that rely on a data aggregator to obtain or process the consumer's financial account and transaction data, the role of the data aggregator may be opaque to the consumer. As consumers increasingly access fintech applications through their mobile devices, the likelihood that they will read and understand long and meticulous disclosures diminishes.

While complex disclosures designed to protect service providers rather than inform consumers are a problem, consumers should make every effort to read disclosures so that they understand their rights and obligations. It is not enough to assert that measures are needed to ensure that consumers understand what they are agreeing to when they use third-party applications. As one observer wrote, "[d]isclosures written in plain language might increase consumer awareness, but

69. A number of the financial planners and investment advisers indicated that it was more difficult to obtain data from 401(k) plans, particularly the smaller ones, than from traditional broker-dealers.

70. See, e.g., General Instruction C.(3).g of Form N-1A under the Securities Act and Investment Company Act (requiring electronic machine-readable information about mutual funds).

that only works if consumers actually read the 'Terms and Conditions' before downloading the latest financial app."[71]

While consumers have to some extent become conditioned to opt for convenience over security, they nevertheless continue to look to their primary financial institutions for protection of their personal and financial data.[72] This raises issues of importance for these financial institutions, including how to verify that their customers have in fact authorized a third party to access their account or initiate a transaction. Further, data aggregators may obtain significantly more consumer financial data than necessary to provide the service that the customer requested, often unknown to the customer. The implications of these features give rise to a potentially wide cascade of issues regarding downstream use of the data, including broader issues related to data privacy that are beyond the scope of this report.

Finally, consumers should have an easy way to revoke their consent to data aggregator access to their financial account and transaction data. Otherwise, data aggregators may retain and continue to use the data and, in some circumstances, may even be able to acquire additional data. It is important that requirements regarding customer authorization be improved to allow customers to exercise control over the scope and duration of data being obtained, how the data is used, and to whom it may be provided.

Recommendations

Treasury recommends that the Bureau work with the private sector to develop best practices on disclosures and terms and conditions regarding consumers' use of products and services powered by consumer financial account and transaction data provided by data aggregators and financial services companies. The goal should be to provide disclosures and terms and conditions that are written in plain language, readily accessible, readable through the preferred device used by consumers to access services, and presented in a reasonably simple and intuitive format so that consumers can give informed and affirmative consent regarding to whom they are granting access, what data is being accessed and shared, and for what purposes. If necessary, the Bureau should consider issuing principles-based disclosure rules pursuant to its authority under Section 1032 of Dodd-Frank.[73]

Treasury also believes that consumers should have the ability to revoke their prior authorization that permits data aggregators and fintech applications to access their financial account and transaction data. Data aggregators and fintech applications should provide adequate means for consumers

---

71. Amber Goodrich, Computer Services, Inc., *5 Challenges of Sharing Consumer Data*, blog post (Nov. 8, 2017), available at: *https://www.csiweb.com/resources/blog/post/2017/11/08/5-challenges-of-sharing-consumer-data*.

72. According to one survey, 91% of U.S. consumers willingly accept the terms and conditions of various mobile applications and services without reading them; for ages 18 to 34 the acceptance rate of terms and conditions, without reading them, is 97%. See Deloitte, *2017 Global Mobile Consumer Survey: US Edition* (2017), at 12, available at: *https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf*. See also A.T. Kearney, *Key Findings from the Consumer Digital Behavior Study* (Apr. 2018), available at: *https://www.atkearney.com/financial-services/the-consumer-data-privacy-marketplace/the-consumer-digital-behavior-study* ("Consumers view banks as their best agent in protecting consumer data privacy and security").

73. See 12 U.S.C. § 5532.

to readily revoke the prior authorization. If necessary, banking regulators and the SEC should consider issuing rules that require financial services companies to comply with a consumer request to limit, suspend, or terminate access to the consumer's financial account and transaction data by data aggregators and fintech applications.

Moving Away from Screen-Scraping to More Secure Access Methods

The practice of using login credentials for screen-scraping poses significant security risks, which have been recognized for nearly two decades.[74] Screen-scraping increases cybersecurity and fraud risks as consumers provide their login credentials to access fintech applications. During outreach meetings with Treasury, there was universal agreement among financial services companies, data aggregators, consumer fintech application providers, consumer advocates, and regulators that the sharing of login credentials constitutes a highly risky practice.

APIs are a potentially more secure method of accessing financial account and transaction data than screen-scraping. A number of foreign jurisdictions have opted to promote access through APIs, in part due to security concerns. The United Kingdom, through its open banking initiative, has specified regulatory standards for data sharing through APIs.[75] The European Union has adopted the Revised Payment Service Directive (PSD2), which requires banks to grant licensed third-party payment service providers access to bank infrastructure and account data. PSD2 also contemplates the standardization of APIs.[76] Singapore has encouraged the use of bank APIs but has not made it a regulatory mandate.[77]

Data aggregators and consumer fintech application providers have expressed reservations with an API approach. They claim, for example, that their efforts to work with financial services companies to do away with screen-scraping have for the most part been met with resistance, and that financial services companies have largely refused to enable direct access to their data or to set up open APIs.[78] There are concerns that without some sort of industry standard or regulatory guidance, API access could be restricted to certain types of data dictated by the financial services company, as opposed to the consumer, susceptible to unexpected interruptions and terminations, and subject to unreasonable and disproportionate liability.

Recommendations

Treasury sees a need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data sharing agreements that effectively

---

74. See footnote 46.

75. Open Banking Ltd., *Guidelines for Read/Write Participants* (ver. 3.2, May 2018), available at: *https://www.openbanking.org.uk/wpcore/wp-content/uploads/Guidelines-for-Read-Write-Participants.pdf*.

76. Directive (EU) 2015/2366 of the European Parliament and of the Council (Nov. 25, 2015), available at: *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN*.

77. Ong Chong Tee, Monetary Authority of Singapore, *The Future of Banking – Evolution, Revolution or a Big Bang?* (Apr. 16, 2018), available at: *http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2018/The-Future-of-Banking.aspx*.

78. See, e.g., Daniel Castro and Michael Steinberg, Center for Data Innovation, *Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help* (Nov. 6, 2017), available at: *http://www2.datainnovation.org/2017-open-apis.pdf*.

move firms away from screen-scraping to more secure and efficient methods of data access. Treasury believes that the U.S. market would be best served by a solution developed by the private sector, with appropriate involvement of federal and state financial regulators.

A potential solution should address data sharing, security, and liability. Any solution should explore efforts to mitigate implementation costs for community banks and smaller financial services companies with more limited resources to invest in technology.

Liability for Unauthorized Access

Screen-scraping also appears tied to the issue of liability. Financial services companies have expressed concerns that they may bear the burden of any losses arising from a breach at the data aggregator or a downstream fintech application. Even if the consumer's losses are not limited by Regulation E,[79] such as when a consumer authorized a person other than the consumer to initiate an electronic funds transfer by providing login credentials to such third party, the consumer may nonetheless expect the bank or other financial institution to make him or her whole for any losses.

Providing login credentials to a data aggregator creates opportunities for bad actors to illicitly obtain such highly sensitive credentials and allow assets to be transferred out of the account. Screen-scraping also can allow a data aggregator to obtain significantly more data than needed by the underlying fintech application, including sensitive personally identifiable information, which could be subsequently stolen.[80] Moving away from screen-scraping can facilitate resolution of the liability issue by eliminating the need for login credentials, reducing the amount and sensitivity of unnecessary data being acquired by data aggregators and decreasing the possibility of an unauthorized transaction.

Some data aggregators have entered into agreements with financial services companies to access the financial account and transaction data through an API but conditioned on contractual liability and indemnification of the financial services company. Other data aggregators have been unable or unwilling to reach agreement on such terms. In such circumstances, data aggregators usually continue to obtain data through screen-scraping.

As the U.S. Government Accountability Office (GAO) has observed, the issue of financial responsibility for consumer losses and access to consumer financial transaction data has been discussed at meetings of federal banking regulators and the Bureau under the auspices of the Federal Financial Institutions Examination Council (FFIEC). However, these discussions have not resulted in any specific policy outcomes to guide market participants.[81] Without resolution of liability and other

---

79. 12 C.F.R. Part 205. Regulation E implements the Electronic Fund Transfer Act, which establishes a framework of the rights, liabilities, and responsibilities of participants in the electronic fund and remittance transfer systems.

80. The sensitivity of consumer financial transaction data can vary. For example, data indicating that a bank account is a checking account may be less sensitive than the associated ABA routing and account numbers. If a fintech application only needs to know the account type, then it would be unnecessary to obtain the more sensitive ABA routing and account numbers.

81. U.S. Government Accountability Office, *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight* (Mar. 2018) at 54-57, available at: *https://www.gao.gov/assets/700/690803.pdf* ("GAO Fintech Report"). GAO reported that some regulators indicated that they had not taken more steps to resolve the disagreements surrounding financial account aggregation because they are concerned over acting too quickly. Id. at 56.

issues, "consumers could have to choose between facing potential losses or not using what they may find to be an otherwise valuable financial service, and fintech firms providing useful services to consumers will face barriers to providing their offerings more broadly."[82]

Recommendations

Treasury recommends that any potential solution discussed in the prior recommendation also address resolution of liability for data access. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.

Standardization of Data Elements

There are other areas in which collaboration among market participants could improve consumers' ability to use their data. Collaborative attempts have been made among financial services companies, data aggregators, and consumer fintech application providers to create standardized data elements, including efforts by Open Financial Exchange (OFX) and Financial Services Information Sharing and Analysis Center (FS-ISAC).[83] However, these efforts have not achieved full consensus to date. A standardized set of data elements and formats would help to foster innovation in services and products that use financial account and transaction data, because it may be more efficient to develop a single agreed-upon taxonomy. Data elements would need to be developed for a broad range of products and services related to banking, investments, retirement, loans, insurance, and taxes. Standardization could improve the market efficiency for financial products and services by making it easier to engage in comparative analysis.

Data currently obtained by aggregators from separate financial services companies can be incompatible and must be cleaned and standardized before it can be used. Financial services companies often use "disparate and customized formats to send and share information, employing different nomenclature for [otherwise] common terms."[84]

Recommendations

Treasury recommends that any potential solution discussed in the prior recommendation address the standardization of data elements as part of improving consumers' access to their data. Any solution should draw upon existing efforts that have made progress on this issue to date. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.

Clarifying When Data Aggregators Are Subject to Third-Party Guidance

Some banks have raised concerns over whether third-party guidance may apply if a bank enters into an API agreement with a data aggregator that establishes terms of access, because the bank has

82. Id. at 57.

83. See footnote 50.

84. Conrad Sheehan, Accenture, *To Capitalize on Open Banking, the Industry Needs Standards*, American Banker (Apr. 10, 2018), available at: *https://www.americanbanker.com/opinion/to-capitalize-on-open-banking-the-industry-needs-standards*.

entered into a contract.[85] Third party guidance clearly applies when a bank itself is providing data aggregation as a service to its customers and has hired a data aggregator to collect the data with its customer's authorization because the data aggregator becomes a service provider to the bank. But when the data aggregator has entered into an API agreement with the bank where it is not providing a service to the bank, it is unclear whether third party guidance may still apply.

Data aggregators would not consider themselves service providers to banks when, for example, they rely on screen-scraping to access financial account and transaction data that has been authorized by a consumer.[86] However, if data aggregators were to instead enter into an API agreement with a bank, it may become subject to third-party guidance because of the contractual relationship, which can increase compliance costs.

This regulatory uncertainty over the application of third-party guidance may, therefore, be inadvertently discouraging more API agreements between banks and data aggregators.

Recommendation

Treasury recommends that the banking regulators remove ambiguity stemming from the third-party guidance that discourages banks from moving to more secure methods of data access such as APIs. Further discussion of bank regulatory oversight of third-party relationships is addressed in the following chapter on Aligning the Regulatory Framework to Promote Innovation.

Current Regulation of Data Aggregators

The greater the amount of consumer financial account and transaction data that is retained by data aggregators, the greater is the possible harm to consumers that could result from a data breach.[87] Although data aggregators do not have a specific regulatory scheme similar to banks or other depository institutions, they are currently subject to regulation under the federal consumer protection laws administered by the FTC as well as state consumer protection laws.[88] Some financial services companies have suggested that the absence of the same level of regulatory oversight of data aggregators and downstream consumer fintech application providers raises significant risks for consumers.[89] In particular, they have argued that the security practices of data aggregators are not comparable to the standards applied at banks and the security practices of consumer fintech application providers are even weaker.

---

85. Banking regulators have issued guidance for assessing and managing risks in third-party relationships. The guidance views a third-party relationship as "any business arrangement between a bank and another entity, by contract or otherwise."

86. Treasury is aware that some data aggregators have entered into agreements with banks, sometimes on an informal basis, while engaging in screen-scraping. For example, a data aggregator may agree to pull the data during the night in order to minimize disruption to the bank's computer systems.

87. In outreach meetings with Treasury, data aggregators have asserted that they mitigate data breach risk by only retaining aggregated and anonymized data that is not associated with any personally identifiable information of the consumer.

88. To the extent that a data aggregator or consumer fintech application provider is providing services to a bank, the services provided are subject to the third-party oversight framework imposed by banking regulators under the Bank Services Company Act.

89. American Bankers Association, *Fintech – Promoting Responsible Innovation* (May 2018), at 3-4, available at: *https://www.aba.com/Advocacy/Documents/fintech-treasury-report.pdf*.

Data aggregators and consumer fintech application providers are subject to the Gramm-Leach-Bliley Act (GLBA),[90] which is a federal law specifying the ways that financial institutions, including some nonbank financial institutions, protect the security and confidentiality of nonpublic personal information of individuals.[91] The provisions in GLBA govern how financial institutions, as defined under the statute,[92] implement administrative, technical, and physical safeguards to insure the security and confidentiality of customer records, protect against any anticipated threats or hazards, and protect against unauthorized access.[93] Financial institutions must explain their policies to their customers that are designed to safeguard sensitive data.[94] These provisions of GLBA are enforced by the FTC, the federal banking agencies, the SEC, and the Commodity Futures Trading Commission (CFTC). To be compliant with GLBA, financial institutions must apply specific protections to customers' private data in accordance with the institution's data security plan.

To implement GLBA, the FTC set forth the primary information security provisions in its Safeguards Rule.[95] The FTC's Safeguards Rule requires financial institutions to assess and develop a documented security plan that describes the company's program to protect customer information, including the following areas particularly important to information security: employee management and training, information systems, and detecting and managing system failures.[96] The intent of the GLBA information security requirements in the Safeguards Rule is to protect consumers and reduce reputational damage caused by unauthorized sharing or loss of private customer data. The FTC has indicated that data aggregators and consumer fintech application providers significantly engaged in financial services and products are financial institutions under GLBA and therefore subject to the Safeguards Rule.[97]

In addition, there are efforts underway to regulate consumer-authorized data aggregation, including potential legislation, at the state level. However, Treasury believes that state-by-state regulation, which would be more cumbersome and costly to comply with as compared with regulation by a single federal regulator, would not be workable given the complexity of data issues at hand.

Recommendation

Moving away from screen-scraping and eliminating the sharing of login credentials will address the most significant concerns raised about the need to increase regulation of data aggregators and

90. Public Law No. 106-102 [codified at 15 U.S.C. Ch. 94]. Also known as the Financial Services Modernization Act of 1999.

91. 15 U.S.C. § 6801(a).

92. Financial institutions include companies that offer consumer financial products or services like loans, financial or investment advice, or insurance.

93. 15 U.S.C. § 6801(b).

94. Id. § 6803(c)(3).

95. 15 U.S.C. §§ 6801, 6805(b); 16 C.F.R. Part 314.

96. 16 C.F.R. §§ 314.3 and 314.4.

97. Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule* (Apr. 2006), available at: *https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (stating that the Safeguards Rule applies to companies that receive information about the customers of other financial institutions)*.

consumer fintech application providers. While data security concerns will remain an important issue, the Safeguards Rule appropriately addresses such concerns.[98]

To the extent that any additional regulation of data aggregation is necessary, Treasury recommends that it occur at the federal level by regulators that have significant experience in data security and privacy, and that will have, through legislation if necessary, broad jurisdiction to ensure equivalent treatment in the nonfinancial sector.

Data Security and Breach Notification

Data Security Standards

The data security provisions of GLBA are enforced by the federal banking agencies for depository institutions,[99] the SEC and the CFTC for entities under their jurisdiction, and the FTC for all other financial institutions.[100] With the exception of the FTC, these federal agencies are authorized to routinely supervise and examine for compliance with these provisions of GLBA and their implementing regulations. These agencies all maintain authority to implement regulations for GLBA.

Data security standards are significantly different between nonfinancial companies, such as retailers and manufacturers, and financial institutions. Vast amounts of consumer payment credentials and financial data are routinely stored on a nonfinancial company's internal or third-party systems, used for marketing purposes, or simply used to complete transactions instantly. Yet, nonfinancial companies are not subject to comprehensive federal data security standards under GLBA and are not subject to routine examination for compliance with data security standards. The only heightened obligation to protect data comes from the exercise of the FTC's authority under Section 5 of the Federal Trade Commission Act[101] to bring enforcement actions against nonfinancial companies for unfair or deceptive practices. The FTC has exercised this authority more than 60 times since 2002; however, this authority is limited to enforcement action and does not give the FTC supervision and examination rights over these nonfinancial companies.[102]

In addition to federal standards, nonfinancial companies and financial institutions subject to the FTC's jurisdiction under GLBA must comply with applicable state laws that impose heightened or specific data security standards. To date, only 13 states have imposed data security standards for protection of consumer financial data, which have different requirements. For instance, Florida requires a business to take "reasonable measures" to protect and secure personal information data

98. In addition to the information security requirements, GLBA also contains privacy requirements as to how financial institutions collect, use, and maintain nonpublic personal information and under what circumstances that information can be shared. These provisions are applicable to financial institutions under the Bureau's Regulation P [12 C.F.R. Part 1016].

99. See Interagency Guidelines Establishing Information Security Standards, as codified at 12 C.F.R. Part 30, App. B (OCC); 12 C.F.R. Part 208, App. D-2 and Part 225, App. F (Federal Reserve); and 12 C.F.R. Part 364, App. B (FDIC).

100. Insurance data security was examined in the Asset Management and Insurance Report.

101. 15 U.S.C. § 45(a)(1).

102. Federal Trade Commission, *Privacy & Data Security Update: 2017*, available at: *https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf*.

that is stored in "electronic form," but Utah does not differentiate between personal information stored electronically or on paper.[103]

Over the last several years, many nonfinancial companies have been subject to significant data breaches of consumer financial data. For example, in 2013, Target announced that payment card information of 41 million consumers was compromised.[104] In 2014, Home Depot announced that the payment card information of more than 50 million customers was stolen in a data breach.[105] More recently, the retailer Hudson's Bay Co. advised roughly 5 million customers of its subsidiary stores Lord & Taylor and Saks Fifth Avenue that their payment credentials had been compromised.[106] Data breaches are not unique to nonfinancial companies and have affected financial institutions as well.[107]

Data Breach Notification

The United States does not have a national law establishing uniform national standards for notifying consumers of data breaches, or for providing them a clear and straightforward mechanism for resolving disputes.[108] In the absence of uniform national standards, states have been aggressive in developing their own data breach notification laws. Each state law may apply to any company located in that state or that does business with residents of that state. In practice, this means that in the event of a data breach companies could be subject to the data breach notification laws of 50 states as well as of the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands.[109] State laws for data breach notification often include specific provisions regarding the number of affected individuals that will trigger notification requirements, the timing of notification, and form of notification, among other requirements. Unsurprisingly, state data breach notification laws are far from uniform. Indeed, they vary in a number of significant ways, including with respect to the most fundamental aspect, namely the scope of data covered under the definition of personal

103. Compare Fla. Stat. § 501.171(2) with Utah Code § 13-44-201.

104. Target Brands, Inc., *Press Release – Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores* (Dec. 19, 2013), available at: *https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car*.

105. The Home Depot, *News Release – The Home Depot Reports Finding in Payment Data Breach Investigation* (Nov. 6, 2014), available at: *http://ir.homedepot.com/news-releases/2014/11-06-2014-014517315*.

106. Mike Murphy, *Saks, Lord & Taylor Data Breach May Affect 5 Million Customers*, MarketWatch (Apr. 1, 2018), available at: *https://www.marketwatch.com/story/saks-lord-taylor-data-breach-may-affect-5-million-customers-2018-04-01*.

107. For example, JPMorgan Chase was subject to a data breach in 2014 and Equifax suffered a data breach in 2017.

108. Federal banking regulators have adopted guidance for depository institutions in the event of unauthorized access to customer information. See Interagency Guidance on Response Programs for Unauthorized Access to Customer information and Customer Notice [70 Fed. Reg. 15736 (Mar. 29, 2005)].

109. National Conference of State Legislatures, *Security Breach Notification Laws* (Mar. 29, 2018), available at: *http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx*.

information.[110] Other inconsistencies among states' breach notification laws can make compliance difficult for firms and entail disparate treatment for consumers. The lack of uniformity and efficiency affects both nonfinancial companies and financial institutions.

Recommendation

Congress has considered establishing a federal data security standard and breach notification standard on several occasions. For example, during the 114th Congress, two separate bills, sharing many common principles, successfully passed their respective committees.[111] During this Congress, legislation has again been considered to establish these federal standards.

Treasury recommends that Congress enact a federal data security and breach notification law to protect consumer financial data and notify consumers of a breach in a timely manner. Such a law should be based on the following principles:

- Protect consumer financial data
- Ensure technology-neutral and scalable standards based on the size of an entity and type of activity in which the entity engages
- Recognize existing federal data security requirements for financial institutions
- Employ uniform national standards that preempt state laws

Digital Legal Identity

Digital identity products and services hold promise for improving the trustworthiness, security, privacy, and convenience of identifying individuals and entities, thereby strengthening the processes critical to the movement of funds, goods, and data as the global economy races deeper into the digital age. Digital identity systems also have the potential to generate cost savings and efficiencies for financial services firms. For instance, trustworthy digital identity systems could improve customer identification and verification for onboarding and authorizing account access, general risk management, and antifraud measures.

Legal Identity

Legal identity is distinct from broader concepts of personal and social identity. Legal identity is the specification of a unique natural or legal person that (1) is based on certain pre-specified characteristics or attributes of the person that are intended to establish the person's uniqueness, (2) is recognized by the state under national law, and (3) ascribes legal rights and duties to that person. Proof of legal identity is required to open a bank, brokerage, or other account at a regulated financial institution. Digital legal identity uses electronic means to unambiguously assert and authenticate a real person's unique legal identity.

110. For example, Maryland specifically includes biometric data of an individual such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristics, while other states do not. Compare Md. Code Com. Law § 14-3501(d) [as amended by House Bill 974 (May 4, 2017)] with Nevada Rev. Stat. § 603A.040.

111. Data Security Act of 2015, H.R. 2205, 114th Cong.; Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong.

Portability

Digital identity systems potentially allow legal identity to be portable. Portable legal identity means the individual's verified identity credentials can be used to establish legal identity for new customer relationships at unrelated financial institutions or government entities, without each financial institution's having to obtain and verify personally identifiable information (PII) to meet regulatory requirements. Portability requires developing interoperable digital identification products, systems, and processes. While not permitted in the private sector under current regulations, trustworthy portable third-party digital identity services could potentially save relying parties time and resources in identifying, verifying, and managing customer identities, including for account opening and access. Portability could also potentially save customers the inconvenience of having to prove and authenticate identity for each unrelated financial institution or government service, and reduce the risk of identity-theft stemming from the repeated exposure of PII.

Components of a Digital Identity System

Digital identity systems may rely on various types of technology and use digital technology in several ways,[112] but generally involve two essential components: (1) identity proofing, enrollment, and credentialing; and (2) authentication. They may also involve a third component, federation, which is optional, but allows identity to be portable. Identity proofing and enrollment may be digital or documentary, remote, or in-person. Credentialing, authentication, and federation are always digital. Different identity service providers can provide some or all of the components of a digital identity system.

Identity proofing establishes that a subject is who they claim to be. It involves obtaining and verifying that attribute evidence is genuine and accurate, and issuing a digital credential to bind the verified identity to a real-life person. Identity proofing depends on official government registration and documentation/certification, or at least on governmentally recognized registration and certification, for verification.[113]

Authentication establishes that the person asserting identity is who he or she claims to be. It involves confirming, through a secure digital authentication protocol, that the individual asserting identity is in control of the technologies and credentials that bind the validated identity to a real person. Successful authentication provides reasonable, risk-based assurances to the relying party that the subject asserting identity today is the same person who previously

112. For example, digital identity systems may use electronic databases to obtain and confirm attribute information and/or store and manage records; digital credentials to authenticate identity for accessing mobile, online, and offline financial activities; and digital biometrics to provide attributes to identify and/or a credential to authenticate individuals.

113. National Institute of Standards and Technology, *Digital Identity Guidelines – Enrollment and Identity Proofing Requirements*, NIST Special Publication 800-63A (June 2017), available at: *https://pages.nist.gov/800-63-3/sp800-63a.html* ("NIST 800-63A").

asserted identity and accessed a financial service, and is in fact a given identified customer. Trustworthy authentication is key for combating account-access identity fraud.[114]

Federation involves the use of federated identity architecture and assertions to convey the results of an authentication process and, if requested or required, attribute information to relying parties across a set of networked systems.[115]

The National Institutes of Standards and Technology (NIST) of the U.S. Department of Commerce has recently established risk-based technical standards for each of the component processes of a digital identity system (enrollment and identity proofing; authentication and lifecycle management; and federation),[116] which are mandatory for the federal government, but only voluntary for the private sector.

Public-Private Roles

Both the government and the private sector have important roles in establishing a trustworthy U.S. digital identity ecosystem. In the United States, the private sector is generally relied upon to develop innovative identity products, services, and business models, while the federal government is ultimately responsible for establishing the minimum substantive requirements for proving legal identity, including core attributes and acceptable attribute evidence. Federal and state government authorities also provide the official government registration and the related official root identity evidence (e.g., birth certificates, passports) on which legal identity currently depends.

Public and private sector stakeholders need to work together to develop trustworthy digital legal identity products and services for use in the financial sector and elsewhere. To facilitate this objective, stakeholders should address a number of issues, including:

- How to leverage the NIST guidelines to establish flexible, risk-based standards for digital customer identification and verification, keyed to the risk levels associated with specific customers and/or types of financial products and services
- How to ensure the trustworthiness, privacy, and cybersecurity of identity service providers, such as government or industry certification and supervision
- Business models and liability allocation appropriate for establishing portable legal identity
- Ways the public and private sectors can effectively work together to reduce regulatory burden and catalyze the market for trustworthy digital identity products and services

114. National Institute of Standards and Technology, *Digital Identity Guidelines – Authentication and Lifecycle Management*, NIST Special Publication 800-63B (June 2017), available at: *https://pages.nist.gov/800-63-3/sp800-63b.html* ("NIST 800-63B").

115. National Institute of Standards and Technology, *Digital Identity Guidelines*, NIST Special Publication 800-63-3 (June 2017), at 14-15, available at: *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf* ("NIST 800-63-3").

116. See NIST 800-63A, 800-63B, and NIST 800-63-3. The NIST digital identity guidelines set requirements for three different levels of trustworthiness, called levels of assurance (LOAs), for each of these component processes, based on the LOA's degree of trustworthiness.

Treasury recommends that financial regulators work with Treasury to enhance public-private partnerships to identify ways government can eliminate unintended or unnecessary regulatory and other barriers and facilitate the adoption of trustworthy digital legal identity products and services in the financial services sector. This would include engaging the private sector to help the financial regulators adopt regulation in the legal identity space that is flexible, risk-, principles-, and performance-based, future-proofed, and technology-neutral. Treasury also recognizes that the development of digital legal identity products and services in the financial services sector should be implemented in a manner that is compatible with solutions developed across other sectors of the U.S. economy and government.

Treasury also supports the efforts of the Office of Management and Budget to fully implement the long-delayed U.S. government federated digital identity system. Treasury recommends policies that would restore a public-private partnership model to create an interoperable digital identity infrastructure and identity solutions that comply with NIST guidelines and would reinvigorate the role of U.S. government-certified private sector identity providers, promoting consumer choice and supporting a competitive digital identity marketplace. Treasury also seeks to leverage the U.S. government federated identity system — in particular, its certification and auditing regime for digital identity providers — to permit financial institutions to use digital identity services provided by certified providers to conduct customer identification and verification for onboarding.

Finally, Treasury encourages public and private stakeholders to explore ways to leverage the REAL ID Act[117] driver's license regime — particularly, robust state REAL ID license identity-proofing processes — to provide trustworthy digital identity products and services for the financial sector.

The Potential of Scale

The ongoing digital transformation of the financial services system is being driven not only by developments in computing power, the expanding ubiquity and interconnection of computers and mobile devices, and the exponential growth in digitized financial data, but also by technologies that can benefit from advances in data and computing capacity at greater scale and with greater efficiency. Scalable technologies such as cloud computing enable financial services companies to store and process vast amounts of data and to quickly add new computing capacity to meet changing needs. At the same time, advances in big data analytics, machine learning, and artificial intelligence are expanding the frontiers of financial services firms' abilities to glean new and valuable business insights from vast datasets.

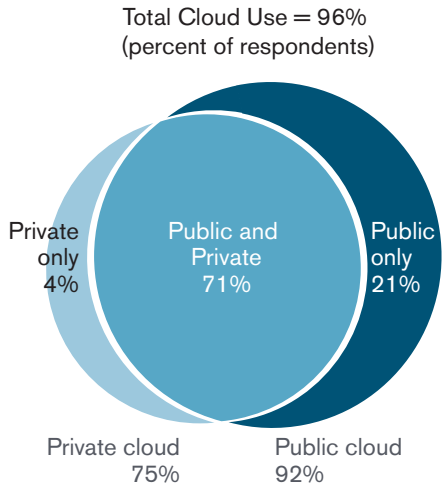
Cloud Technology and Financial Services

Cloud technology is enabling organizations across the economy to more rapidly innovate by reducing barriers to entry to acquire high quality computing resources. Cloud computing, more specifically, enables more convenient, on-demand access to computing resources (e.g., networks, servers,

117. Public Law No. 109-13.

storage, applications, and services).[118] Cloud computing can be deployed through several models: a public cloud, which refers to when these computing resources are available in a shared environment, accessible by multiple customers of the cloud service provider; a private cloud, which refers to when these computing resources are dedicated for use by a single firm, but provided generally in the same type of convenient, rapid, on-demand manner; or a hybrid cloud, which refers to an arrangement consisting of a mix of cloud deployment models.

Figure 5: Cloud Adoption (percent of respondents)



Source: RightScale *2018 State of the Cloud Report.*

Before the broad availability of a public cloud, only large organizations with ample budgets were able to cover the costs involved with building out large-scale internal information technology (IT) infrastructures. Firms would have to make large capital expenditures on computing and networking hardware as well as maintain ongoing operating expenses for multiple layers of software and large IT staffs. With public cloud services, however, firms of all sizes can essentially lease a range of computing resources and expertise from cloud service providers, potentially at lower cost.

Several large technology-focused firms have been central to the development of cloud computing, and the growth of the public cloud market in particular. To achieve the scale necessary to maximize the potential of this technology requires substantial resources. For this reason, these firms continue to dominate the market though competition has increased. The adoption of public cloud is occurring throughout the economy with, for example, survey data suggesting that some 92% of

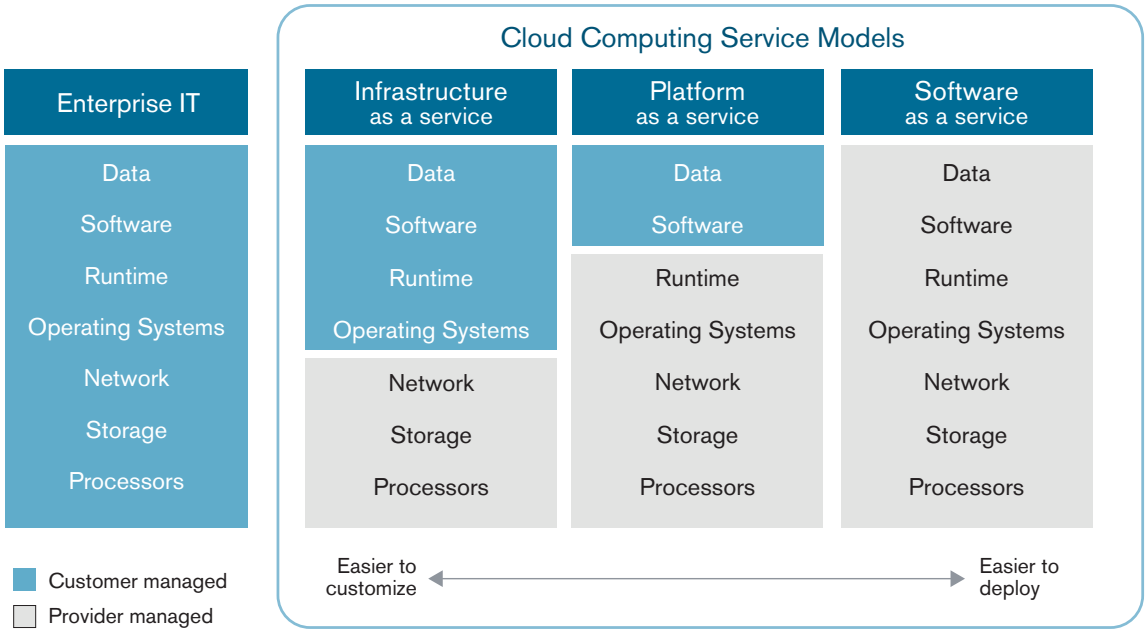
118. National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (Sept. 2011), at 2-3, available at: *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf*.

businesses adopting at least some form of public cloud services.[119] Other sources forecast robust growth in public cloud revenues[120] and data usage.[121]

Types of Cloud Services

While traditional IT often requires firms to manage computing resources internally, cloud computing is generally provided under three service models that provide varying degrees of outsourcing and customization. Infrastructure-as-a-service (IaaS) gives clients the greatest overall control of function and scale by allowing them to expand processing, storage, networks, and other essential

Figure 6: Traditional IT Compared to Cloud Computing



Source: Adapted from U.S. Department of Transportation, *Uses of Cloud Technology for Geospatial Applications*

119. RightScale, Inc., *RightScale 2018 State of the Cloud Report* (2018).

120. One market observer forecasts global public cloud revenue growing from $153.5 billion in 2017 to $186.4 billion in 2018, a 21.4% increase. See Gartner, Inc., *Press Release – Gartner Forecast Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018* (Apr. 12, 2018), available at: *https://www.gartner.com/newsroom/id/3871416*.

121. Cisco estimates, by 2021, 95% of global data center traffic will come from cloud services and applications. Annual global cloud traffic will reach 19.5 zettabytes (ZB) by the end of 2021, up from 6.0 ZB in 2016. One ZB is equal to sextillion bytes, or one trillion gigabytes. See Cisco, *Cisco Global Cloud Index: Forecast and Methodology 2016-2021* (2018), available at: *https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf*.

Figure 7: NIST Definition of Cloud Computing

Essential characteristics	On-Demand Self-Service	User can unilaterally provision server time, network storage, etc. as needed without involving service provider.
	Broad Network Access	Capabilities are available over the network and accessed through common mechanisms (e.g. a Web browser) and devices.
	Resource Pooling	Physical and virtual resources are shared across a large pool of users, allowing for dynamic assignment according to users' demands.
	Rapid Elasticity	Computing capabilities can be scaled rapidly up or down according to users' demands, such that any given user's demand is met without interruption.
	Measured Service	Users access capabilities as a service and pay only for resources used.
Service models	Software-as-a-Service (SaaS)	End-user applications provided as a service only. User cannot manage or control any underlying cloud infrastructure.*
	Platform-as-a-Service (PaaS)	Application platforms or middleware provided as a service on which users can build and deploy custom applications using programming languages, libraries and other tools supported by service provider.
	Infrastructure-as-a-Service (IaaS)	Broad and scalable computing capabilities provided as a service, including processing, storage, networks, and operating systems, enabling more control over deployed applications.
Deployment models	Public Cloud	The cloud infrastructure is available for open use by the general public. It generally is owned by and exists on the premises of the cloud service provider.
	Private Cloud	The cloud infrastructure is available for exclusive use by a single organization. It may exist on or off premises and may be owned by the organization, a third party, or both.
	Community Cloud	The cloud infrastructure is available for use only by a specific community of users that have shared needs or concerns. It may be owned by one or more of the community users, by a third party, or some combination.
	Hybrid Cloud	The cloud exists as a configuration of two or more distinct cloud infrastructures (public, private, or community) that enables data and application portability among the separate infrastructures.

* Cloud infrastructure includes network, servers, data, middleware, operating systems, storage, etc.

Source: National Institute of Standards and Technology.

computing resources on-demand as needed.[122] In contrast, software-as-a-service (SaaS) allows clients to easily use a cloud provider's software that runs on the cloud infrastructure,[123] but tends to provide users the least flexibility or customization. Platform-as-a-service (PaaS) models, which

122. Other service models are sometimes described by industry participants – for example, business-process-as-a-service and data-as-a-service – but generally these can be seen as variants of SaaS, PaaS, or IaaS models.

123. NIST further describes "cloud infrastructure" as consisting of the physical systems (for example, server, storage and network components) and software applications that enable the essential cloud characteristics.

includes elements of IaaS, provides clients control over the deployment and configuration of software applications, but without any control over the underlying cloud hardware/infrastructure.

Adoption in Financial Services

Financial institutions have been adopting cloud computing in part because of the benefits it provides in effectively managing a firm's IT and computing resources.[124] Many firms have chosen to deploy private cloud or hybrid cloud structures to gain the benefits of cloud while also retaining greater control of their IT in order to satisfy regulatory or other requirements.[125] For certain uses, however, financial institutions are also adopting public cloud, including for tasks and processes that are susceptible to surges in required computing power. This can include volatile workloads associated with periodic stress testing, risk modelling and simulations, or other requirements where computing resources may need to rapidly scale (e.g., payments).

All three types of cloud service models are also being deployed within financial services. SaaS, because it tends to be the easiest to deploy, has the most widespread uptake across financial institutions.[126] SaaS platforms can easily handle, for example, customer relationship management and commercial lending software, as well as noncore services such as e-mail, payroll, billing, and human resources that are amenable to outsourcing. Financial institutions are generally more likely to utilize IaaS and PaaS service models to run more complex or enterprise-specific core services and applications — including treasury, payments, retail banking, and regulatory functions.

Overall, the financial services sector has reportedly been slower to adopt cloud computing than other industries, though this appears to be changing. Industry research suggests that a significant proportion of financial organizations still support much of their IT infrastructure in-house rather than through a cloud service provider.[127] Banks, for example, have been slow to migrate core activities for a number of reasons, including the criticality of such functions and the difficulty of transitioning away from legacy IT systems. However, expectations are for cloud adoption to increase for the financial services sector, just as with other sectors of the economy. Some analysts

---

124. In a May 2017 whitepaper, the Depository Trust & Clearing Corporation noted that the many relative benefits of cloud contributed to its decision to "strategically expand" the range of services and applications it runs using cloud technology, asserting that cloud computing "has reached the tipping point as the capabilities, resiliency and security of services provided by cloud vendors now exceed those of many on-premises data centers." See Depository Trust & Clearing Corporation, *Moving Financial Market Infrastructure to the Cloud* (May 2017), available at: *http://perspectives.dtcc.com/media/pdfs/13161-Cloud-WhitePaper-05-11-17.pdf*.

125. Filip Blazheski, BBVA Research, *Cloud Banking or Banking in the Clouds?* (Apr. 29, 2016), available at: *https://www.bbvaresearch.com/wp-content/uploads/2016/04/Cloud_Banking_or_Banking_in_the_Clouds1.pdf*.

126. Id.

127. In a 2016 study, Peak 10, an IT consultancy (reorganized as Flexential in January 2018), found that 75% of financial services firms still support technology infrastructure in-house. See Peak 10, *Financial Services and IT Study: Tackling the Digital Transformation* (2016), available at: *http://www.peak10.com/2016-financial-services-and-it-study/*; Flexential, *Financial Services Cloud Adoption: Top Concerns for Making the Move*, blog post (May 2018), available at: *https://www.flexential.com/knowledge-center/blog/financial-services-cloud-adoption-top-concerns-making-move*.

expect large U.S. banks to process the vast majority of their computing needs on cloud platforms within the next 5-10 years.[128]

Issues and Recommendations

Overall Benefits and Potential Risks

Cloud computing has helped increase the speed of innovation by allowing firms to more efficiently and rapidly deploy computing resources to meet business demands and extract usable insights from large datasets.

Scalability, Speed, and Cost

Cloud computing, by enabling financial institutions to rapidly scale up or down their use of cloud applications and infrastructure, provides an efficient way to meet changing demands for computing power and enhances firms' abilities to bring new products and capabilities to market. In a traditional enterprise IT environment, procuring a single new server, for example, could take months to obtain necessary approvals and cost thousands of dollars. In contrast, cloud computing can enable firms to acquire the same computing resources in minutes and potentially at a fraction of the cost.

For new and smaller firms, the economies of scale and affordable cost structure of cloud are key factors in allowing firms to provide products at a scale, quality, and speed that they might otherwise be unable to achieve. Large firms, too, benefit from using cloud because of the sheer volume or resources and magnitude of the economies of scale available through large cloud service providers.

Security and Resilience

Large cloud service providers typically have the resources and expertise to invest in and maintain state-of-the-art and comprehensive IT security and deploy it on a global basis across their platforms. Financial institutions, especially small and mid-sized firms, could find it economically infeasible to achieve similar levels of security on their own. Moreover, because cloud service providers can rapidly re-distribute data across geographically diverse storage and processing centers, cloud environments can potentially enhance firms' strategies for business continuity and operational resilience. Nevertheless, to maintain these advantages in terms of security and resilience, cloud service providers must constantly guard against the risks of being targeted by bad actors.

Enabling Large-Scale Data Storage and Management

Critically, cloud enables the computing resources that are increasingly required by firms that must manage or utilize vast volumes of data, whether for regulatory purposes or in order to build and maintain competitive advantages. Firms in the financial services industry can leverage powerful machine learning and other data analytics tools to analyze large data sets with greater agility and effectiveness in line with firms' business models and strategies. These tools can potentially be used to comb through mountains of text-based documents, generate know-your-customer identity

128. Keith Horowitz et al., Citi Research, *U.S. Banks: Transformational Changes Unfolding in Journey to the Cloud* (Jan. 10, 2018).

maps by conducting pattern of life analytics, and convert voice-based input into text and insights about sentiment and intent.

The growth of cloud services also presents certain challenges, including potentially high transitioning costs, security and data privacy considerations, regulatory compliance standards, unrealized or over-sold cost savings compared to in-house IT management, and connectivity speed. Further, firms may face high switching costs if they seek to change cloud service providers and may find themselves with little pricing power relative to the large providers. However, many of these challenges can be addressed through appropriate adaptation of cloud computing services, such as deployment of a private or hybrid cloud, choice of service model, provision of data availability and resilience measures, and other appropriate risk management of outsourcing contracts.

Regulatory Challenges in Adoption

Regulatory compliance issues continue to present challenges to the broader adoption of and migration to cloud technology by financial services firms. Cloud Security Alliance, an industry group, reported in March 2015, for example, that 71% of respondents to a survey on cloud adoption by financial services firms cited "regulatory restrictions" as a key reason, second only to "data security concerns" that was cited by 100% of respondents, for why they had not yet adopted cloud technology.[129]

Financial services firms face several regulatory challenges related to the adoption of cloud, driven in large part by a regulatory regime that has yet to be sufficiently modernized to accommodate cloud and other innovative technologies. The large number of regulators involved with allowing the use of cloud in financial services can present administrative burdens, as well as challenges with inconsistent requirements. Inconsistencies in regulators' experience with cloud computing and in the knowledge base at the examiner level may also be a contributing factor.[130]

Regulatory Outsourcing Guidelines

Financial institutions continue to seek certainty from regulators with regard to permissible uses of public cloud services, and some have indicated that they are hesitant to adopt or migrate to cloud services due in part to regulatory guidance that is either inconsistent or unclear or not well adapted for cloud services. For example, firms have expressed uncertainty over whether regulators' third-party service provider guidance applies to all or only some cloud deployment models (IaaS, PaaS, and SaaS). Firms are also uncertain as to whether regulators would accept a broader migration to

129. Cloud Security Alliance, *How Cloud is Being Used in the Financial Sector: Survey Report* (Mar. 2015), at 10, available at: *https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud_Adoption_In_The_Financial_Services_Sector_Survey_March2015_FINAL.pdf*.

130. See Securities Industry and Financial Markets Association, *Promoting Innovation in Financial Services* (Apr. 6, 2018), at 37-38 (submission to Treasury).

the cloud for core activities, because financial services firms manage highly sensitive and important customer data and perform critical functions for the economy.[131]

Some of the regulatory guidance may also not be well adapted to cloud. Compliance with regulatory guidance that requires financial institutions to maintain physical access audit rights, for example, can present challenges, including the ability of financial institutions to negotiate on-site access, given a cloud service provider potentially has hundreds or thousands of clients. In the case of vendor audit requirements, industry and market participants have suggested that U.S. financial regulators seek to incorporate independent U.S. audit and certification standards for cloud service providers, which may provide more efficient, consistent and useful means of assessing such services.

Further, these regulatory issues may have implications for a bank's relationship with a third party that itself uses a cloud service provider (i.e., a fourth party). These "chain outsourcing" issues can present challenges to banks looking to partner with third parties that use cloud services.

Data Localization

Data stored on the cloud can easily be moved and stored anywhere. Cloud computing is not naturally geo-centric; rather, data can be compartmentalized, moved, and processed wherever there is available storage and processing capacity. These capabilities, however, do not necessarily impede the ability of U.S. financial regulators to maintain access to regulated entities' electronic books and records for monitoring, surveillance, and other regulatory purposes, including during a financial crisis. Nevertheless, some jurisdictions have imposed requirements that mandate that data be stored or processed within national borders — so-called localization requirements – or considered such requirements.[132] Data localization can have unintended and harmful effects on competition, innovation, and economic growth. Concerns about data security and access can be better addressed through technology, enhanced security controls, contractual arrangements, and bilateral or multi-jurisdictional agreements.

Outdated Record Keeping Rules

Certain rules prescribe technology requirements that may be out of date or that unnecessarily hinder adoption of new technologies such as cloud computing. Rule 17a-4 under the Securities Exchange Act of 1934,[133] for example, requires any electronic media used by broker-dealers to be

131. Ongoing work by industry groups and other public-private sector partnerships can perhaps be instructive in helping regulators achieve harmonization, within and across jurisdictions, of standards and requirements to provide greater regulatory certainty. The work of the NIST Cloud Computing Standards Roadmap Working Group, an industry-academia-regulatory collaboration, is one such effort. See National Institute of Standards and Technology, *NIST Cloud Computing Standards Roadmap*, Special Publication 500-291, Version 2 (July 2013), available at: *https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf*.

132. There are limited examples of such restrictions today in the United States. Section 9.3.15.7 of Internal Revenue Service Publication 1075 requires that any agency using external information system services to process, store, or transmit federal tax information "restrict the location of [such systems] to areas within the United States territories, embassies, or military installations." See Internal Revenue Service, *Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information* (Sept. 2016), at 95, available at: *https://www.irs.gov/pub/irs-pdf/p1075.pdf*.

133. 17 C.F.R. § 240.17a-4

stored under the "Write Once, Read Many" or "WORM" format. In effect, the rule compels firms to record and store static snapshots of data, which can be more costly and potentially less secure than employing more dynamic data storage capabilities.

Recommendations

Treasury recognizes that cloud computing is a key technology with the potential to allow financial institutions to significantly enhance their ability to innovate, better serve businesses and consumers, and compete both domestically and abroad.

Treasury recommends that federal financial regulators modernize their requirements and guidance (e.g., vendor oversight) to better provide for appropriate adoption of new technologies such as cloud computing, with the aim of reducing unnecessary barriers to the prudent and informed migration of activities to the cloud. Specific actions U.S. regulators should take include: formally recognizing independent U.S. audit and security standards that sufficiently meet regulatory expectations; addressing outdated record keeping rules like SEC Rule 17a-4; clarifying how audit requirements may be met; setting clear and appropriately tailored expectations for chain outsourcing; and providing staff examiners appropriate training to implement agency policy on cloud services.

Treasury further recommends that a cloud and financial services working group be established among financial regulators so that cloud policies can benefit from deep and sustained understanding by regulatory authorities. Financial regulators should support potential policies by engaging key industry stakeholders, including providers, users, and others impacted by cloud services. Separately, Treasury encourages private industry cloud services providers to proactively formulate standards appropriate for the United States that might address the potential risks presented by the growing use of cloud technology.

Financial regulators in the United States should seek to promote the use of cloud technology within the existing U.S. regulatory framework to help financial services companies reduce the risks of noncompliance as well as the costs associated with meeting multiple and sometimes conflicting regulations.[134] Regulators should be wary of imposing data localization requirements and should instead seek other supervisory or appropriate technological solutions to potential data security, privacy, availability, and access issues.

134. This should also include development of information and communications technology standards to improve the interoperability and portability of the cloud. In cloud computing, interoperability refers to the ability of different systems or components, such as those of a financial services company and a cloud services provider, to exchange and use information or to otherwise work together successfully, while portability refers to the ability to move and adapt applications and data between systems, including the different cloud deployment models or the systems of other cloud services providers. Recent E.U. action has sought to make progress in this area. See European Commission, *FinTech Action Plan: For a More Competitive and Innovative European Financial* Sector (Mar. 8, 2018), available at: *http://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0001.02/DOC_1&format=PDF*.

Big Data, Machine Learning, and Artificial Intelligence in Financial Services

The application of artificial intelligence (AI) to a wide array of uses across the economy,[135] including financial services, has greatly increased over the past few years. The concept of AI can vary meaningfully, but generally is associated with efforts to enable machines or computers to imitate aspects of human cognitive intelligence, such as vision, hearing, thinking, and decision making. AI and machine learning algorithms have powered many innovations across the broader economy, spanning the power of internet search engines, facial-recognition software, and the potential for autonomous cars.

One of the primary sub-branches of AI development is known as machine learning. Machine learning generally refers to the ability of software to learn from applicable data sets to "self-improve" without being explicitly programmed by human programmers. The nature of "improvement" in the software would depend on the specific machine learning use-case, but could include the quality of image-recognition, the ability to more accurately and efficiently identify money laundering, or the ability to accurately predict fraud, borrower default, or the most useful web links in response to a set of search terms. In general, the more data available for the machine learning models, the better such models will perform because of their ability to learn from the examples in an iterative process referred to as "training the model."

Machine learning has been around in some form since at least the 1940s and advanced rapidly in recent years.[136] It can span several categories: classical machine learning, which would include supervised learning (focusing on advanced regressions and categorization of data that can be used to improve predictions) and unsupervised learning (processing input data to understand the distribution of data to develop, for example, automated customer segments); and deep and reinforcement learning (which is based on neural networks, and may be applied to unstructured data like images or voice).[137]

Several interrelated developments in technology have enabled this environment:

- Dramatic improvements in the availability and affordability of computing capacity through, for example, cloud computing and the general improvements in computer hardware.
- An explosion in the abundance of digitized data and its analysis, sometimes referred to as "big data." Consider that by 2020, digitized data is forecasted to be generated at a level that is more than 40 times the level produced in 2009.[138] In 2012, it was estimated that 90% of the digitized data in the world had been generated in just the prior two years.[139]

---

135. Ananad Rao, *A Strategist's Guide to Artificial Intelligence*, Strategy + Business (Summer 2017), available at: *https://www.strategy-business.com/article/A-Strategists-Guide-to-Artificial-Intelligence*.

136. See id.

137. Marko Kolanovic and Krishnamachari Rajesh, J.P. Morgan Securities LLC, *Big Data and AI Strategies: Machine Learning and Alternative Data Approach to Investing* (May 2017).

138. A.T. Kearney, *Big Data and the Creative Destruction of Today's Business Models* (2013), at 2, available at: *https://www.atkearney.com/documents/10192/698536/Big+Data+and+the+Creative+Destruction+of+Today s+Business+Models.pdf/f05aed38-6c26-431d-8500-d75a2c384919* (discussing Oracle forecast).

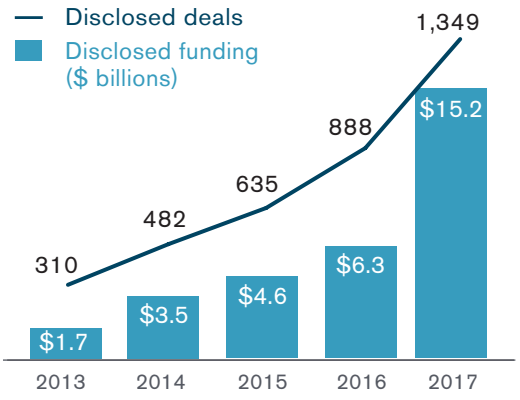
139. Id.

Since 2012, more than a billion more people have been added to the internet (2.5 billion people connected to the internet in 2012 compared to 3.7 billion people in 2017).[140]

- The proliferation of mobile devices and other internet connected devices (e.g., wearable devices, household appliances, components in industrial production), sometimes referred to as the "internet of things." Globally, there are an estimated 27 billion devices (including smartphones, tablets, and computers) currently connected to the internet, with expectations for 125 billion connected devices by the year 2030.[141] These devices are enabling new streams of data that are being used by businesses to effectively digitize many dimensions of interaction in our physical world. Information from cars, phones, cameras, watches, manufacturing plants, are all being collected and available for analysis.

These factors are highly interwoven. The sheer magnitude of data that is now available demands analytical tools, like AI, to capably process and make use of the vast amounts of information, which is only expected to accelerate in volume, velocity, and variety. In some use-cases, for example, manual processes are simply unusable given the amount of data that exists. Cloud service providers, recognizing that many cloud-service users are also in need of adequate analytical tools, are providing various services designed to enable users to deploy an array of AI capabilities.[142]

Figure 8: Global Investment Trends in Artificial Intelligence



Source: CBInsights, *Top AI Trends to Watch in 2018*, at 25.

Deployment in Financial Services

Investment in AI and machine learning has been accelerating over the past several years with a large share of such investment focused on firms looking to deploy AI and machine learning in financial services. Adoption of AI within financial services is driven by a number of factors such as the large and growing availability of data within financial services, including through third-party consumer financial data aggregators discussed elsewhere in this report, and the expectation that the use of machine learning and AI will increasingly be a driver of competitive advantage for firms through both improving firm's efficiency by reducing costs and enhancing the quality of financial services products demanded by

140. Id.

141. IHS Markit, *The Internet of Things: A Movement, Not a Market* (Oct. 2017), at 2, available at: *https://cdn.ihs.com/www/pdf/IoT_ebook.pdf*. For projections that do not consider computers and phones at: Gartner, Inc., *Press Release – Gartner Says 8.4 Billion Connected "Things" Will be in Use in 2017, up 31 Percent from 2016* (Feb. 7, 2017), available at: *https://www.gartner.com/newsroom/id/3598917*.

142. See, e.g., Amazon Web Services, *Amazon Machine Learning Documentation*, available at: *https://aws.amazon.com/documentation/machine-learning/*; Microsoft Azure, *Azure AI: Artificial Intelligence Productivity for Virtually Every Developer and Scenario*, available at: *https://azure.microsoft.com/en-us/overview/ai-platform/*; Google Cloud, *Cloud Machine Learning Engine*, available at: *https://cloud.google.com/ml-engine/*; and IBM, *AI, Machine Learning and Cognitive Computing Services*, available at: *https://www.ibm.com/services/artificial-intelligence.*

customers.[143] Global banks, for example, report they expect application of these tools to deliver long-term cost efficiencies, risk management benefits, and revenue expansion opportunities.[144]

An extensive array of AI and machine learning use-cases are being considered and deployed within financial services, spanning the front-end (customer-facing) to back-office operations of a broad-set of financial services activities. These use-cases include:[145]

Risk mitigation and surveillance: Financial institutions and regulators, for example, are using machine learning-enabled software to help conduct surveillance of trader behavior by combining transaction data and unstructured text (e.g., e-mail, messaging) and voice data to help identify suspicious trading activities.[146] Machine learning may additionally be used to help reduce fraud and conduct surveillance for money-laundering and other illicit financing risks. Financial regulators are also beginning to employ machine learning to enhance their own analysis and understanding of economic and financial markets.[147]

Enhancing investment analysis, trading strategies, and operations: Machine learning-based software can also be used to augment human investment analysis in a variety of ways. One firm's product allows users to ask simple text questions (like an internet search engine) to generate instant correlation analyses between a broad span of potential market-moving data and financial asset prices, which could be used to greatly accelerate investment analyses.[148] Other use-cases include optimizing trade execution[149] and portfolio management and trading strategies at quantitative-oriented asset managers and hedge funds.[150]

---

143. PricewaterhouseCoopers, *Top Financial Services Issues of 2018* (Dec. 2017), available at*: https://www.pwc.se/sv/pdf-reports/finansiell-sektor/top-financial-services-issues-of-2018.pdf (*discussion of artificial intelligence and digital labor).

144. Laura Noonan, *AI in Banking: The Reality Behind the Hype*, Financial Times (April 12, 2018) ("Noonan AI in Banking").

145. For further examples, see Lex Sokolin, Autonomous NEXT, #*Machine Intelligence & Augmented Finance: How Artificial Intelligence Creates $1 Trillion of Change in the Front, Middle and Back Office of the Financial Services Industry* (Apr. 2018); Michael Chui et al., McKinsey Global Institute, *Notes from the AI Frontier: Applications and Value of Deep Learning* (Apr. 2018), available at: *https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-applications-and-value-of-deep-learning*; Darrell West and John R. Allen, Brookings Institution, *How Artificial Intelligence is Transforming the World* (Apr. 2018), available at: *https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/*.

146. Tony Sio, Nasdaq, *Changing the Game: Artificial Intelligence in Market Surveillance*, blog post (Apr. 2017), available at: *http://business.nasdaq.com/marketinsite/2017/Changing-The-Game-Artificial-Intelligence-In-Market-Surveillance.html.*

147. See, e.g., Andrew Haldane, Bank of England, *Will Big Data Keep Its Promise?* (Apr. 2018), available at: *https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/will-big-data-keep-its-promise-speech-by-andy-haldane.pdf*.

148. See Antoin Gara, *Wall Street Tech Spree: With Kensho Acquisition S&P Global Makes Largest A.I. Deal In History*, Forbes (Mar. 6, 2018), available at: *https://www.forbes.com/sites/antoinegara/2018/03/06/wall-street-tech-spree-with-kensho-acquisition-sp-global-makes-largest-a-i-deal-in-history/*.

149. See Laura Noonan, *JPMorgan Develops Robot to Execute Trades*, Financial Times (July 31, 2017)

150. See Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications* (Nov. 1, 2017), at 18, available at: *http://www.fsb.org/wp-content/uploads/P011117.pdf*.

Customer-interface: Many financial services firms are employing chat-bots, which are digital customer-facing assistants that are powered by machine learning software that takes advantage of advancements in natural-language processing. For example, customers can text message with a bank through a messaging platform (and voice as well) in a conversational style to engage in certain account services. While current services are fairly limited in U.S. applications, expectations are that these systems will evolve to enable a much richer set of customer-facing services.[151]

Underwriting decisions: Firms have begun to employ machine learning based models to assist in underwriting decisions for purposes of extending credit to consumers and small businesses. Insurance firms are also using these techniques to price and market insurance products.

While many of these efforts remain in the early stages of testing and deployment, several use-cases appear poised for more wide-spread adoption. Within the banking industry, for example, large percentages of U.S. banks report either current or planned AI deployment within the next 18 months across the following use-cases: more than 60% in biometrics, about 60% in fraud & security detection, about 55% in chatbots or robo-advisers; and about 35% in voice assistants.[152]

Issues and Recommendations

The expected rapid adoption of AI and machine learning within the financial services industry, and the economy more broadly, raises a number of important policy considerations.

Benefits and Risks from Competition in AI and Big Data

Firms expect that the effective use of AI, machine learning and big data analysis will be a key source of competitive advantage, which is spurring investment and competition.[153] Smaller firms may now be able to compete providing new algorithms, in part because barriers to develop such software have declined with the availability of affordable data processing capacity. Traditional financial services players may be able to leverage their product expertise while technology firms may be able to leverage their experience and deployment in AI in other contexts. Investment managers may look to employ new data sources or tools to deliver improved relative investment performance.[154] This multi-faceted competition can provide benefits to end-users and consumers of financial services through more affordable and higher-quality products that are more personalized and provided with greater overall convenience. The development of AI is expected to yield substantial benefits

151. Brian Patrick Eha, *This is How Financial Services Chatbots are Going to Evolve*, American Banker (May 26, 2017), available at: *https://www.americanbanker.com/news/this-is-how-financial-services-chatbots-are-going-to-evolve.*

152. See Citigroup Global Markets Inc., *Bank of the Future: The ABCs of Digital Disruption in Finance* (Mar. 2018) (citing Business Insider Intelligence, *AI in Banking and Payments* (Feb. 2018)).

153. PricewaterhouseCoopers, *Artificial Intelligence and Digital Labor in Financial Services*, available at: *https://www.pwc.com/us/en/industries/financial-services/research-institute/top-issues/artificial-intelligence.html (last accessed June 1, 2018)* (noting that about half (52%) of those in the financial services industry said they are currently making "substantial investments" in AI and that almost three out of four (72%) business decision makers expect that AI will be the business advantage of the future).

154. Tammer Kamel, Quandl, *Alternative Data – The Trend in Financial Data*, blog post (Apr. 12, 2016), available at: *https://blog.quandl.com/alternative-data* (discussing why alternative data can provide a source of potential 'alpha' for investment professionals).

to the broader economy and financial services.[155] PricewaterhouseCoopers estimated that by 2030, AI technologies could increase North American gross domestic product (GDP) by $3.7 trillion and global GDP in $15.7 trillion.[156] Within the financial services sector, large banks report that AI could help cut costs and boost returns.[157]

The strength and nature of the competitive advantages created by advances in AI could also harm the operations of efficient and competitive markets if consumers' ability to make informed decisions is constrained by high concentrations amongst market providers. Some analysts caution that the path of AI-based financial services technology may be similar to the path of other technology-based platforms that have trended toward high-levels of market concentration (e.g., in internet search and messaging).[158] An AI/machine learning model's performance improves through an abundance of data. Models that have a large market presence, therefore, have a built-in self-reinforcing advantage as their gains in market share improve the model's performance, which could in turn further their gain in market share.

Legal and Employment Challenges

As the implications of the wide-spread adoption of AI become clearer, responsible parties are sounding alarms on potential complex downside risks.

Detecting versus promoting fraud: Even as AI and machine learning tools are being used to help detect fraud through risk models and image-recognition software, other applications of this technology could be used to circumvent fraud detection capabilities. For example, the digital rendering of fraudulent videos and audios may become indistinguishable from actual video and audio, which would raise significant challenges to authentication and verification functions within financial services.[159]

Compatibility of legal and algorithmic decision-making: One advantage of machine learning and AI methods is that they can potentially help avoid discrimination based on human interactions by ceding aspects of such decision making to an algorithm. However, these methods may also risk discrimination through the potential to compound existing biases, through training models with biased data and the identification of spurious correlations.[160] One consideration will be to ensure that decisions based upon an algorithm do not rely on incorrect, or perhaps even fraudulent, data,

---

155. McKinsey Global Institute, *Artificial Intelligence: The Next Digital Frontier* (June 2017), available at: *https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/how-artificial-intelligence-can-deliver-real-value-to-companies (*discussing the potential value of AI in other sectors of the economy).

156. PricewaterhouseCoopers, *Sizing the Prize: What's the Real Value of AI for Your Business and How Can You Capitalise*? (2017), available at: *https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf*.

157. See Noonan AI in Banking.

158. See, e.g., Sokolin.

159. Penny Crosman, *Bank of America, Harvard Form Group to Promote Responsible AI*, American Banker (Apr. 10, 2018), available at: *https://www.americanbanker.com/news/bank-of-america-harvard-form-group-to-promote-responsible-ai*.

160. See, e.g., Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (2016); Mikella Hurley and Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 Yale J. L. & Tech. 148 (2016).

or alternatively base decisions on proxies for illegal discrimination. Another key consideration is the appropriate role of humans in a decision-making process informed by algorithms that may be unable to provide an adequate explanation of its decision-making process nor self-correct for biases built into the data or model design.[161]

Employment risks and opportunities: Financial services firms expect the widespread adoption of AI and robotic automation processes to create significant demand for employees with applicable skills in AI methods, advanced mathematics, software engineering, and data science. However, executives also expect the application of these technologies to result in potentially significant job losses across the industry.[162]

Data Privacy

The deployment of AI and machine learning models could result in a higher overall quality of financial services products being delivered to consumers. At the same time, the ubiquity and continuous flowing nature of data required to train AI and machine learning models can raise various data protection and privacy concerns. As data becomes ubiquitous, consumer's financial and nonfinancial data may be increasingly shared without their understanding and informed consent. Moreover, the power of AI and machine learning tools may expand the universe of data that may be considered sensitive as such models can become highly proficient in identifying users individually.[163]

Regulatory Challenges Related to Transparency, Auditability, and Accountability

In the lending context and many other financial services use-cases, the underlying complexity of AI and machine learning-based models (often referred to as "black boxes") raises challenges in the transparency and auditing of these models. Many U.S. laws or regulations have been designed around a baseline expectation of auditability and transparency that may not be easily met by these models. As these types of models are deployed in increasingly high-value decision-making use-cases, such as determining who gets access to credit or how to manage an investment portfolio, questions regarding how to maintain accountability become fundamental.

With respect to lending, for example, U.S. rules require that a creditor provide a notification when a borrower has been denied credit.[164] In light of the increasing complexity of machine learning, it can be challenging to express the underpinnings of these analytical insights to firms, borrowers, and regulators.[165]

---

161. See Nick Bostrom and Yudkowsky Eliezer, *The Ethics of Artificial Intelligence*, The Cambridge Handbook of Artificial Intelligence (Keith Frankish and William M. Ramsey, eds., 2014).

162. See Noonan AI in Banking.

163. *The Future: The Sunny and Dark Side of AI*, The Economist (Mar. 31, 2018).

164. Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion?* (Jan. 2016), at 14, available at: *https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf*.

165. Eva Wolkowitz and Sarah Parker, Center for Financial Services Innovation, *Big Data, Big Potential: Harnessing Data Technology for the Underserved Market* (2015), available at: *https://s3.amazonaws.com/cfsi-innovation-files/wp-content/uploads/2017/02/13062352/Big-Data-Big-Potential-Harnessing-Data-Technology-for-the-Underserved-Market.pdf*.

In the investment management context, for example, machine learning-based algorithms and alternative data sources are currently being deployed in financial markets by a subset of quantitative-oriented funds, with the expectation of increased adoption by other such funds. While the application of these tools could yield valuable investment insights for some investment portfolios and activities, the opacity of the models may raise challenges for supervisors and users of these models to monitor risk and understand how they may interact with one another, particularly in times of broad market stress.[166]

Recommendations

Treasury recognizes that the increased application of developing AI and machine learning technologies can provide significant benefits by improving the quality of financial services for households and businesses and supplying a source of competitive strength for U.S. firms. Regulators, therefore, should not impose unnecessary burdens or obstacles to the use of AI and machine learning and should provide greater regulatory clarity that would enable further testing and responsible deployment of these technologies by regulated financial services companies as the technologies develop.

The Administration has made harnessing AI and high-performance computing, including machine learning and autonomous systems, a federal research and development priority.[167] In May 2018, the White House hosted a summit of more than 100 senior government officials, technical experts, and business leaders to discuss policies to support continued American innovation in AI across industrial sectors.[168] Participants at the summit, including Treasury, recognized the importance of enabling high-impact, research and development efforts to advance AI. Treasury recommends that financial regulators engage with the Select Committee on Artificial Intelligence,[169] in addition to pursuing other strategic interagency AI efforts. Engagement in such efforts should emphasize use-cases and applications in the financial services industry, including removing regulatory barriers to deployment of AI-powered technologies. Other potential issues to consider as part of that engagement include: an appropriate emphasis on human primacy in decision making for higher-value use-cases relative to lower-value use-cases, the importance of cost-benefit assessments for regulatory actions, preparation of the work force for the trend toward digital labor, transparency of model use for consumers, robustness against manipulation (e.g., in market contexts), and accountability of human beings.

---

166. See Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications* (Nov. 1, 2017), at 18 and 33-34, available at: *http://www.fsb.org/wp-content/uploads/P011117.pdf*.

167. Office of Management and Budget, *Fiscal Year 2019 Analytical Perspectives*, at 236, available at: *https://www.whitehouse.gov/wp-content/uploads/2018/02/spec-fy2019.pdf*.

168. 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), available at: *https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf*.

169. The Select Committee is chaired by the White House Office of Science and Technology Policy, the National Science Foundation (NSF), and the Defense Advanced Research Projects Agency (DARPA). Senior federal officials participating on the Select Committee include the Undersecretary of Commerce for Standards and Technology, the Undersecretary of Defense for Research and Engineering, the Undersecretary of Energy for Science, the Director of NSF, and the Directors of DARPA and the Intelligence Advanced Research Projects Activity as well as representatives from the National Security Council, the Office of the Federal Chief Information Officer, and the Office of Management and Budget.

Aligning the Regulatory Framework to Promote Innovation

Overview

Technological innovation in the provision of financial services is creating opportunities to serve customers and markets more efficiently. However, the regulatory framework, for banks and nonbanks alike, must evolve to enable innovation on an orderly and sustainable basis. Nonbank financial service providers generally operate within a largely state-based regulatory regime requiring compliance with a disparate set of standards across individual states and territories that can be cumbersome and produce conflicting guidance for entities operating on a national basis.[170]

Innovation will best flourish if the current federal and state regulatory models evolve to keep pace with technological change. This evolution could include efforts by the states to harmonize their regulatory and supervision regimes; the Office of the Comptroller of the Currency's (OCC) special purpose national bank charter; and encouragement of the bank partnership model with fintech firms.

As financial services continue to be shaped by new technologies and business models, the traditional distinctions between permitted banking activities and other information-intensive digital activities are being tested, which will require flexible and effective regulatory approaches. Existing bank regulations and supervision of a broad spectrum of third-party technology service providers and relationships require additional attention to enable innovative partnerships and provide for more streamlined and tailored oversight.

Challenges with State and Federal Regulatory Frameworks

State Oversight and Harmonization Challenges

State laws and regulations currently provide the primary regulatory framework for many types of nonbank financial services firms, including firms deploying new and innovative technologies and products. State banking departments and financial regulatory agencies oversee various types of nonbank firms and activities, including: consumer finance companies, money services businesses (MSBs), debt collection businesses, and mortgage loan originators. State financial regulators' authorities over these nonbank firms can include firm licensing requirements; safety and soundness regulation, including permissible investments and required reserves; product limitations; interest rate limits; examinations; and enforcement authority for violation of state and federal laws.

Lending and Servicing

State financial regulators regulate nonbank consumer lenders primarily for purposes of consumer protection. Nonbank lenders that operate in multiple states must acquire lending or credit licenses for each applicable state. As a result, geographic expansion can only generally be accomplished through repeated licensing efforts, each with a state-specific regulatory regime. States' lending

170. With the passage of Dodd-Frank, the Bureau of Consumer Financial Protection was granted expansive federal regulatory powers over nonbank financial services companies, but Dodd-Frank did not preempt state laws that provided greater consumer protection. See 12 U.S.C. § 5551(a).

license applications often require submission of a business plan and financial statements, credit reports and fingerprints from the firm's officers, and a surety bond. State regulators oversee lenders active across a broad set of consumer lending segments, including short-term, small dollar, mortgage, auto, and other unsecured credit.

State-specific requirements would benefit from additional harmonization. For example, some states may require a physical office presence,[171] some require broker licenses or licenses for commercial loans,[172] and others set different maximum loan interest rate requirements.[173] Differences in usury limits imposed by states also materially impact which products are available to consumers.

Payments and Money Transmission

Money transmitters are generally nonbank firms that transfer or receive funds on behalf of individuals. As with nonbank credit providers, individual states each license and supervise money transmitters with the general goals of maintaining the safety and soundness of these businesses, ensuring financial integrity, protecting consumers, and preventing ownership of money transmitters for illicit purposes (e.g., money laundering or fraud). The definition of money transmission can vary significantly by state (as can exceptions from the definition), posing operational challenges and potentially chilling economically beneficial money transmission activity —— particularly innovative, technology-based money transmission. If a statutory exception does not apply, money transmitter licenses are required for numerous activities offered by nonbanking firms beyond just remittance services, to firms that could include online payment, digital wallet services, and bill payment services.[174]

As a general matter, any firm with a nationwide footprint (and especially those that have only a digital presence) will require a license in, and be subject to examination by, every state in which it operates. There are currently 49 states plus the District of Columbia and Puerto Rico that impose some sort of licensing requirement in order to engage in the business of money transmission or money services. As with lending and credit, money transmitter licensing requirements often vary by state, but generally include requirements to submit credit reports, business plans, and financial statements; and a requirement to maintain a surety bond to cover losses that might occur. Some states may also ask for information regarding policies, procedures, and internal controls. These

171. Arizona, Hawaii, Missouri, North Carolina, Nevada, South Carolina, and Texas require a physical office to obtain a license as a mortgage lender or broker.

172. California, New York, and Vermont require a license for commercial lenders, while most states only require a license for consumer loans.

173. See Loanback.com, *Usury Laws by State* (Mar. 2, 2011), available at: *http://www.loanback.com/category/usury-laws-by-state*.

174. Money transmitters are defined for federal purposes by FinCEN for purposes of the Bank Secrecy Act, 31 U.S.C. § 5311 et seq. Money transmitters generally include any person that provides money transmission services or is engaged in the transfer of funds. The term money transmission services means the acceptance of currency, funds, or other value that substitutes for currency and transmission to another location or person by any means. Money transmitters are considered to be a type of "money services business" (MSB). MSBs are certain nonbank financial institutions that do business in any of the following capacities: money transmitter; currency dealer or exchange, check casher, provider or seller of prepaid access, issuer or seller of traveler's checks, or money orders; U.S. postal service. See 31 C.F.R. § 1010.100(ff).

requirements do not apply to banks because state money transmitter statutes generally expressly carve them out.[175]

Focus Areas for Improvement in the Regulatory Framework

Nonbank firms have raised concerns with the lack of regulatory harmonization among the current state-based regimes, particularly with respect to the provision of credit and money transmission activities. As innovation allows firms to more easily serve customers across a broad national market, these concerns are becoming more acute. The lack of harmonization could also perpetuate a disparate regulatory regime between nonbanks and banks otherwise competing in similar product and geographic markets.[176]

State licensing processes can create inefficiencies, including requirements for fingerprinting in multiple states (although this has been improved through coordination) and requests from states for the financial statements of the multinational parent company's individual board members. The applications for licenses require similar but sufficiently distinct information that forces firms to materially revise each application for each state.

Compliance across this fragmented state-regulatory landscape can be costly for firms (some firms report that all-in licensing costs range from $1 million to $30 million), separate and beyond the time lost from such efforts, which can result in forgone business opportunities.[177] In addition to these up-front costs, nonbank firms must actively monitor regulatory requirements across all the states in which they operate, pay fees to the applicable state regulators, and deploy significant resources to accommodate multiple state examinations, which can result in as many as 30 different state regulators per year examining a firm.[178] These cumulative challenges of operating in the state-based regulatory regime result not only in excessive regulatory costs, but also constrain the ability of nonbank firms, including start-ups, to innovate and to scale nationally.

Banks and credit unions also face regulatory challenges that may impede innovation. In contrast to the largely state-based regime facing nonbank financial services providers, banks and credit unions operate within a largely federal regulatory regime, which provides for greater levels of uniformity, and accordingly efficiency, on some dimensions. Yet banks face a substantially different regulatory regime, which is heavily focused on bank-specific activities. These regulations are structured to ensure the safety and soundness of the bank or credit union, and may include capital and liquidity standards, deposit insurance requirements, and limitations on permissible activities. This regulatory framework exists for multiple reasons, including the need to protect taxpayers because of banks' access to Federal Deposit Insurance Corporation (FDIC) insurance and the Federal Reserve's discount window. Additionally, banks and credit unions serve as the back-up source of

175. Each state may have different statutory language. See, e.g., National Conference of Commissioners on Uniform State Laws, *Uniform Money Services Act* (Feb. 25, 2005), at § 103(4), available at: *http://www.uniformlaws.org/shared/docs/money%20services/umsa_final04.pdf*.

176. For a discussion of how state-based regulation can result in inefficiency, unlevel competition, and differences in the availability of financial services across states, see Brian Knight, *Federalism and Federalization on the Fintech Frontier*, 20 Vanderbilt J. of Ent. & Tech. Law 129 (2017), at 185-198.

177. GAO Fintech Report, at 45.

178. Id.

liquidity for other financial firms, act as critical (though not exclusive) transmission vehicles for monetary policy, and have exclusive access to Fedwire and other payment systems.

The cumulative impact of these regulations, while critical for achieving public policy goals such as safety and soundness, can impede innovation at banking organizations. These limitations may impede the ability of banks and credit unions to partner with nonbank financial institutions, develop new platforms within the organization, or offer new and innovative services to customers.

Modernizing Regulatory Frameworks for National Activities

Improving the Clarity and Efficiency of Our Regulatory Operating Models

Treasury has identified several principles for updating the regulatory operating models available for firms in our financial services ecosystem. First, modernization needs to focus on producing efficient regulation to enable dynamic innovation. Second, any solution must provide sufficient flexibility to recognize the diversity of the scale, maturity, and activities of firms. Finally, any solution should recognize the benefits of both federal and state based-approaches to financial services oversight.

The diversity of U.S. financial services firms requires that any regulatory solution allow for recognition of a broad spectrum of business models. Some firms may be ready to absorb the costs of regulation that attach to a federally insured depository institution, whether through federally chartered banks or state-chartered banks, including traditional banks and industrial loan companies. Other firms may prefer having a primary federal regulatory regime but without the acceptance of federally insured deposits, such as through the OCC's proposed special purpose national bank charter. Still other firms may desire to partner with an existing bank, rather than pursue a banking charter themselves. Finally, firms may have business models that do not require national approaches and may prefer therefore to maintain a predominantly state-based system of regulation. Primary drivers of these decisions may include the type of activity engaged in, the maturity of the firm, and business strategies and objectives.

The United States has a long and complex history of state and federal regulation in financial services. The U.S. banking system began through state charters. In many ways, the state-based system acts as a laboratory of innovation for firms, which should be preserved. In fact, the state model has allowed for numerous nonbank firms to build a local product in a state, and then subsequently expand as the product gained broader market appeal. State regulators also have greater proximity to their constituents and can be more responsive to the needs and preferences of local consumers than regulators who do not have a local presence. Some of these advantages of local geographic experimentation and local government responsiveness should be preserved, particularly for firms that prefer the state-based approach.

Federal oversight would likely play a more prominent role in the regulation of fintech firms if these firms elect to pursue a banking charter. Federal banking regulations should be appropriately tailored to allow firms to provide financial services to drive economic growth while ensuring appropriate oversight. Thought should also be given to the appropriate regulatory structure taking into

consideration organizational structure, services provided, risk profile, and the need to promote fair competition between different types of organizations providing similar services.

A Tailored Regulatory Solution

Treasury supports several specific regulatory approaches that would provide greater clarity and flexibility in the regulatory operating model for firms looking to provide financial services. Taken together, these approaches balance the key requirements for modernizing the regulatory operating model for U.S. firms. These approaches include:

- State Harmonization. An acceleration in state regulators' and legislatures' efforts to harmonize the existing patchwork of state licensing and oversight of nonbank financial services companies,
- Bank Charters. The OCC should move forward with thoughtful consideration of applications for special purpose national bank charters,
- Partnerships. Enabling further partnerships between banking organizations and fintech companies, and
- Bank Innovation. Updating existing bank regulations to enable innovations commensurate with the rapid changes in how banks are partnering with and investing in fintech and technology firms and how banks are themselves becoming increasingly like technology firms.

Issues and Recommendations

State Harmonization Efforts

State regulators have enhanced the regulatory efficiency of state regulation over the years. In the early 1980s, state regulators participated in a nationwide licensing system for the securities industry, known as the Central Registration Depository.[179] In the years leading up to nationwide banking, states were already working to move toward a more harmonized system. By 1991, for example, 33 states permitted nationwide banking and 13 permitted regional banking.[180]

Past and current efforts to promote greater state harmonization have spanned efforts to address differences across state laws, for example with regard to licensing and supervision.

Model Law Adoption

One approach for state harmonization involves the drafting of a model law that state legislatures would then enact and implement in each respective state. This would ensure that each state has similar laws and requirements for each type of firm or activity. For example, in July 2017, the Uniform Law Commission approved and recommended for adoption by all states a Uniform

179. Conference of State Bank Supervisors, *Letter to Treasury on NonBank and Innovation Report* (Apr. 9, 2018), available at: *https://www.csbs.org/letter-treasury-non-bank-and-innovation-report* ("CSBS Letter").

180. See U.S. Department of the Treasury, *Modernizing the Financial System: Recommendations for Safer, More Competitive Banks* (Feb. 5, 1991) at 7, available at: *http://3197d6d14b5f19f2f440-5e13d29c4c016cf-96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1990/1991_0205_TreasuryBanks.pdf*.

Regulation of Virtual Currency Businesses Act.[181] The effectiveness of the model law approach turns on widespread adoption by the states. Previous efforts have met with mixed results. For example, the Commission's Money Services Act of 2000 has to date been enacted by only 10 states (plus Puerto Rico and the U.S. Virgin Islands).[182]

Nationwide Multistate Licensing System

In more recent years, state regulators have been focused on developing greater cooperative approaches for the supervision of nonbank financial services companies. One of the primary efforts of state regulators to achieve such enhanced cooperation has been the Nationwide Multistate Licensing System (NMLS), which is a technology platform that functions as a system of record for the licensing activities (application, renew, and surrender) of 62 state or territorial government agencies.[183] The NMLS is used by state regulators to reduce duplicative regulatory requirements, promote greater information sharing and coordination, and maintain consumer protections and the strength and resilience of regulated firms.

The NMLS began with a focus on the mortgage industry. The NMLS began operations in January 2008 and was formed by the Conference of State Bank Supervisors (CSBS) and the American Association of Residential Mortgage Regulators. At that time, the NMLS was originally the Nationwide Mortgage Licensing System and was primarily designed for the mortgage industry. The NMLS began in 2005 as a voluntary system used by seven state agencies and then expanded to 50 when it went live in 2008. Congress subsequently enacted the Secure and Fair Enforcement for Mortgage Licensing Act (SAFE Act), which established a registration requirement and minimum licensing requirements for mortgage loan originators and mortgage reporting.[184]

The CSBS and state regulators further built out the NMLS framework beyond the mortgage industry. For example, the CSBS and state regulators have expanded the scope of industries covered within the NMLS framework beyond even money transmitters, to also include consumer finance and debt collection. Some success has also been found using NMLS to manage licensing. As of year-end 2017, 38 states were using NMLS to manage their MSB licenses.[185] However, fewer state regulators participate in these other licensed activities than for the mortgage sector.[186] Beyond the scope of industries, NMLS has also enabled greater access to its data through the launch of a publicly available consumer access website in 2010 and through the sale of NMLS data to businesses that, in turn, sell data and loan origination products to mortgage market participants.

---

181. National Conference of Commissioners on Uniform State Laws, *Uniform Regulation of Virtual Currency Businesses Act* (July 2017), available at: *http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2017AM_URVCBA_AsApproved.pdf*.

182. See *http://uniformlaws.org/Act.aspx?title=Money%20Services%20Act* (website of the National Conference of Commissioners on Uniform State Laws tracking the status of enactment as of June 1, 2018).

183. State Regulatory Registry LLC, *2017 Annual Report*, available at: *https://nationwidelicensingsystem.org/NMLS%20Document%20Library/2017%20SRR%20Annual%20Report.pdf* ("NMLS 2017 Annual Report").

184. The SAFE Act was enacted as Title V of the Housing and Economic Recovery Act of 2008, Pub. L. No. 110-289, and codified at 12 U.S.C. §§ 5101-5116.

185. National Multistate Licensing System, *Money Services Businesses Fact Sheet* (Dec. 31, 2017), available at: *https://nationwidelicensingsystem.org/about/Reports/2017Q4%20MSB%20Fact%20Sheet.pdf*.

186. NMLS 2017 Annual Report.

Efforts to Streamline Examinations

One example of how states have sought to harmonize examinations has been their approach to money transmitters and MSBs. Multi-state examinations started in earnest after the Money Transmitters Regulators Association (an association of state money transmitter regulators) executed a cooperative agreement in 2002 and an examination protocol in 2010[187] and FinCEN issued an MSB examination manual for the Bank Secrecy Act in 2008. As of March 2018, 48 states; Washington, D.C.; Puerto Rico; Guam; and the Virgin Islands have signed the Money Transmitter Regulators Association agreements.[188] The agreements provide for a taskforce that helps to coordinate the joint exams and determine which state will lead a joint exam. Joint exams generally include fewer than 10 states, and states that are not part of a joint exam will come in to do individual exams (or be a part of a different joint exam). State examiners generally jointly examine for common components such as Bank Secrecy Act/anti-money laundering, information technology, and corporate governance; there is a separate section of the exam for specific state law issues.

Vision 2020 Commitment and Passporting

State regulators have launched a multi-step effort to develop a 50-state licensing and supervisory system by 2020, known as "Vision 2020." Vision 2020 is largely a response to the various state regulatory harmonization challenges raised by firms regarding the current state-based regulatory regime for nonbank financial companies. The core components of this effort include:[189]

- Establishing a Fintech Industry Advisory Panel that would be a vehicle to provide state regulators important insight on the Vision 2020 and related efforts to improve state regulation.
- Re-designing the existing NMLS platform through further automation and enhanced data and analytical tools.
- Harmonizing multistate supervision processes through adoption of best practices and, critically, the development of a comprehensive state examination system that will allow state regulators to share various pieces of information including: exam schedules, ratings, supervisory concerns, and reports of examination. This system is tentatively scheduled to go live in the spring or summer of 2019.[190] For money-transmission oversight, according to the CSBS, "If one state reviews key elements of state licensing for a money transmitter — IT, cybersecurity, business plan, or background check[191] — then other participating

187. Conference of State Bank Supervisors and Money Transmitters Regulators Association, *The State of State Money Service Businesses Regulation and Supervision* (May 2016), at 11, available at: *https://www.csbs.org/sites/default/files/2017-11/State%20of%20State%20MSB%20Regulation%20and%20Supervision%202.pdf*.

188. CSBS Letter, at 15.

189. Conference of State Bank Supervisors, *Vision 2020 for Fintech and Non-Bank Regulation* (Jan. 7, 2018), available at: *https://www.csbs.org/vision2020*.

190. See NMLS 2017 Annual Report, at 15.

191. This effort would also include examinations for compliance with the federal Bank Secrecy Act.

states agree to accept the findings."[192] Seven states have initially signed on to this agreement as an initial pilot program.[193]

- Other efforts to, for example, assist state banking departments and promote greater industry awareness.

One solution that could be accomplished through the Vision 2020 process is the idea of "passporting" and reciprocity of state licenses. Such a solution would involve the states harmonizing licensure and supervision laws and regulations, creating a system whereby a licensee in one state could have their home state's license accepted, or passported, to other states within the reciprocity pact.[194] Passporting represents a path through which states could effectuate a system of licensing that is conducive to a national business model while still retaining oversight at the state level.

Recommendations

State regulators play an important and valuable role in the oversight of nonbank financial services firms. Treasury supports state regulators' efforts to build a more unified licensing regime and supervisory process across the states. Such efforts might include adoption of a passporting regime for licensure. However, critical to this effort are much more accelerated actions by state legislatures and regulators to effectively reduce unnecessary inconsistencies across state laws and regulations to achieve much greater levels of harmonization. Treasury recommends that if states are unable to achieve meaningful harmonization across their licensing and supervisory regimes within three years, Congress should act to encourage greater uniformity in rules governing lending and money transmission to be adopted, supervised, and enforced by state regulators. Congress has used a similar model previously, such as the establishment of minimum mortgage licensing requirements under the SAFE Act.[195]

OCC Special Purpose National Bank Charter

The OCC's special purpose national bank charter, proposed in 2016, presents an attractive option for firms interested in the benefits of having a single primary federal regulator. This type of banking charter may provide a more efficient, and at least a more standardized, regulatory regime, than the current state-based regime in which they operate. The OCC special purpose national bank charter, however, does present key policy and regulatory considerations, discussed below.

---

192. Conference of State Bank Supervisors, *Press Release – State Regulators Take First Step to Standardize Licensing Practices for Fintech Payments* (Feb. 6, 2018), available at*: https://www.csbs.org/state-regulators-take-first-step-standardize-licensing-practices-fintech-payments*.

193. Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas, and Washington.

194. Brian Knight, Mercatus Center, *Modernizing Financial Technology Regulations to Facilitate a National Market*, Mercatus Center (July 2017), at 5, available at: *https://www.mercatus.org/system/files/knight_-_mop_-_modernizing_fintech_regulations_-_v2_1.pdf*.

195. 12 U.S.C. §§ 5104-08

Overview

The OCC released a proposal for a special purpose national bank charter for financial technology companies and solicited comments on that proposal in December 2016. As proposed,[196] the OCC special purpose national bank charter would allow charter applicants that make loans or engage in payments activities to:

- Adhere to a uniform set of national banking rules, rather than seeking state-by-state lending or money transmission licenses, with frequently conflicting requirements, or partnering with a bank to access bank charter benefits (e.g., the ability to export interest rates);
- Operate without FDIC deposit insurance, to the extent applicants would not take deposits; and
- Be subject to the same standards and level of supervision as similarly situated national banks, including capital, liquidity, consumer protection and financial inclusion requirements based on the business model and risk profile of the chartered company.

Marketplace lenders (MPLs) and payment companies are examples of fintech firms that may be interested in applying for the OCC special purpose national bank charter. MPLs may be attracted to an OCC special purpose national bank charter because it would reduce licensing and regulatory cost by consolidating supervision under one primary national regulatory structure, which would allow them to efficiently provide credit to consumers and businesses across the country. Payments companies might look to the charter to obviate the need to obtain money transmission licenses in all 50 states. The charter might also allow them to acquire potentially more efficient access to payment systems, reduce operating costs and provide national scalability.

Chartering Authority

Under the National Bank Act (NBA), the OCC has authority to grant charters for national banks to engage in the "business of banking," which the OCC has interpreted to include at least one of three "core banking functions" — taking deposits, paying checks, or lending money.[197] The OCC

196. The OCC special purpose national bank charter was proposed through a series of OCC announcements. See Office of the Comptroller of the Currency, *Exploring Special Purpose National Bank Charters for Fintech Companies* (Dec. 2016), available at: *https://www.occ.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf*; ("OCC Fintech Paper"); *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective* (Mar. 2016), available at: *https://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-responsible-innovation-banking-system-occ-perspective.pdf*; *Summary of Comments and Explanatory Statement: Special Purpose National Bank Charters for Financial Technology Companies* (Mar. 2017), available at: *https://www.occ.gov/topics/responsible-innovation/summary-explanatory-statement-fintech-charters.pdf* ("OCC Comment Summary"); *Draft Licensing Manual Supplement* (Mar. 2017), available at: *https://www.occ.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf*.

197. See OCC Comment Summary, at 14. See also 12 U.S.C. § 24 (enumerating the powers of a national bank as "all such incidental powers as shall be necessary to carry on the business of banking"); 12 C.F.R. § 5.20(e)(1) ("A special purpose bank that conducts activities other than fiduciary activities must conduct at least one of the following three core banking functions: Receiving deposits; paying checks; or lending money.").

has also exercised its authority to reach technology-based extensions of core-banking functions, such as facilitating programs electronically.[198]

Key Regulatory Features

The OCC special purpose national bank charter could, as proposed, allow for the preemption of certain state laws and trigger baseline supervisory expectations that apply to any national bank including, for example: a business plan that must assess risks comprehensively; capital adequacy; liquidity; compliance risk management; consumer protection and fair lending compliance; financial inclusion; recovery and resolution planning; governance; and Bank Secrecy Act/anti-money laundering requirements.

The OCC could tailor compliance requirements under a special purpose national bank charter to better suit the safety and soundness risks posed by these institutions in light of the absence of FDIC insurance and potential business model differences.

- Insured Deposit Related Differences (CRA, Resolution). An OCC special purpose national bank chartered firm that does not obtain FDIC insurance (an uninsured national bank) would not present a direct risk to taxpayers through the FDIC's Deposit Insurance Fund. Moreover, under the terms of the CRA, such firms would not be subject to CRA requirements, nor be subject to resolution by the FDIC under the Federal Deposit Insurance Act. However, in its policy statement, the OCC noted that it would encourage special purpose national bank charter applicants to meet an ongoing financial inclusion standard of "provid[ing] fair access to financial services by helping to meet the credit needs of its entire community" through setting supervisory expectations and making such a commitment a condition for charter approval.[199] As to resolution, the OCC would, as provided for under the NBA, resolve such an uninsured national bank. The OCC issued a final rule in December 2016 that clarifies the framework for such a resolution.[200]
- Potential Tailoring of Safety and Soundness Rules (Capital, Liquidity). The OCC noted that it would consider adapting capital requirements for an applicant as necessary to adequately reflect the risks of the planned business model as it does with all national banks.
- State Laws and Consumer Concerns. The NBA preempts state usury laws for federally chartered national banks. However, certain other consumer protections and state contract law may apply, including state laws regarding foreclosure.[201]

Other key features of the OCC proposal that would require some clarifications are:

198. OCC's authority on these issues has been challenged in two lawsuits that have been dismissed on ripeness grounds. See *Conference of State Bank Supervisors v. Office of the Comptroller of the Currency*, No. 17-0763, 2018 WL 2023507 (D.D.C. Apr. 30, 2018); *Vullo v. Office of the Comptroller of the Currency*, No. 17-cv-3574, 2017 WL 6512245 (S.D.N.Y. Dec. 12, 2017).

199. See OCC Fintech Paper, at 12; see also 12 C.F.R. § 5.20(f)(1)(ii).

200. The OCC's resolution framework would apply to any type of uninsured national bank that the OCC charters. See Receiverships for Uninsured National Banks (Dec. 15, 2016) [81 Fed. Reg. 92594 (Dec. 20, 2016)].

201. See for example 12 U.S.C. § 7.4008 (non-real estate lending).

- Regulatory Coordination. National banks, including special purpose national banks, are required (with limited exceptions) to become members of the Federal Reserve System. The Federal Reserve would have to assess whether an OCC special purpose national bank would be given access to the Federal Reserve payment systems.[202]
- Activities Incidental to the Business of Banking. The OCC has authority to define what activities are part of the business of banking or incidental to the business of banking.[203] The OCC indicated it would consider the permissibility of new activities for a special purpose national bank charter on a case-by-case basis.[204]

Recommendations

Treasury recommends that the OCC move forward with prudent and carefully considered applications for special purpose national bank charters. OCC special purpose national banks should not be permitted to accept FDIC-insured deposits, to reduce risks to taxpayers. The OCC should consider whether it is appropriate to apply financial inclusion requirements to special purpose national banks. The Federal Reserve should assess whether OCC special purpose national banks should receive access to federal payment services. It is important that a charter not provide an undue advantage to newly chartered firms relative to the banks that have operated within the existing regulatory system for years. Striking the right balance to appropriately enable a tailored regulatory framework is important.

Bank Regulatory Oversight of Third-Party Relationships

Banking regulators' oversight of banking organizations' relationships with third-parties stems from (1) their general safety and soundness authority over the banking organization and (2) the Bank Service Company Act, which grants federal banking regulators authority to examine and regulate the provision of certain services that a third-party service provider, which may include fintech partners, performs for regulated institutions.[205]

This supervisory regime is generally designed to be comprehensive in overseeing how banking organizations interrelate with third-party vendors and service providers.

Banking regulators administer this oversight through:

- Regulation and supervision of banking organizations. This guidance directs banks to have a comprehensive, enterprise risk management process that addresses such third-party relationships (for example ensuring compliance with applicable laws and regulation); and
- Direct supervision of a subset of service providers (significant service providers and regional service providers).[206]

---

202. Governor Lael Brainard, *Where Do Banks Fit in the Fintech Stack* (Apr. 28, 2017), available at: *https://www.federalreserve.gov/newsevents/speech/brainard20170428a.htm*.
203. 12 U.S.C. § 24.
204. OCC Fintech Paper, at 4.
205. 12 U.S.C. § 1867(c).
206. Federal Financial Institutions Examination Council, *Supervision of Technology Service Providers* (Oct. 2012), at 1, available at: *https://ithandbook.ffiec.gov/media/274876/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf* ("FFIEC TSP Handbook").

Critically, a banking organization's use of a third-party service provider does not diminish the responsibility of the bank to ensure that the activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations, just as if the institution were to perform the activities in-house.

Drivers of Third-Party Risk

Technological innovation, specialization, cost, and today's competitiveness all contribute to financial institutions' increased outsourcing to third parties. Some of this outsourcing includes specific functions (e.g., human resources, taxes, law, and information technology), customer related activities, and lines of business. This has led to new forms of risk as financial institutions become more reliant on others to perform business functions, support services, and technology provisioning. For example, as technology providers increase, cyber risks may increase because of the introduction of new vulnerabilities that may be exploited as vectors for intrusions. In recent years, regulators' and firms' attention to third-party risks and relationships have increased for a variety of reasons, including the following:

- Consumer-Related Concerns. Banks have increasingly been held responsible for the sales practices of third parties that marketed products on their behalf.[207] These incidents have heightened the importance of managing third-party risks related to consumer compliance and protecting a firm's reputation.
- Information Security Concerns. Several high profile data breaches have increased attention to cyber risks. In 2014, Target acknowledged that the payment information of 40 million customers, along with up to 70 million customers' personal information, had been breached as the result of a third-party vendor's systems being compromised.[208] In 2013, regulators notified banking customers of a serious data breach that occurred in 2011 at one of the largest payments information processors used by banks, Fidelity National Information Services.[209]
- Other Operational Risks. Dependence on third parties also raises concerns regarding concentration risk, the reliance on a few vendors to enable the execution of critical functions and services, and highlights the need for contingency planning for both the

207. See, for example, Bureau of Consumer Financial Protection, *Press Release – Consumer Financial Protection Bureau Orders Santander Bank to Pay $10 Million Fine for Illegal Overdraft Practices* (Jul. 14, 2016), available at: *https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-orders-santander-bank-pay-10-million-fine-illegal-overdraft-practices/*; Bureau of Consumer Financial Protection, *Press Release – CFPB Orders American Express to Pay $59.5 Million for Illegal Credit Card Practices* (Dec. 23, 2013), available at: *https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-american-express-to-pay-59-5-million-for-illegal-credit-card-practices/*; Bureau of Consumer Financial Protection, *Press Release – CFPB Orders Chase and JPMorgan Chase to Pay $309 Million Refund for Illegal Credit Card Practices* (Sept. 19, 2013), available at: *https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-chase-and-jpmorgan-chase-to-pay-309-million-refund-for-illegal-credit-card-practices/*.

208. Testimony of John Mulligan, Executive Vice President and Chief Financial Officer of Target Corporation, before the Senate Judiciary Committee (Feb. 4, 2014), available at: *https://corporate.target.com/_media/TargetCorp/global/PDF/Target-SJC-020414.pdf*.

209. Tracy Kitten, *OCC: More Third-Party Risk Guidance*, Bank Info Security (Aug. 26, 2014), available at: *https://www.bankinfosecurity.com/occ-more-third-party-risk-guidance-a-7233*.

financial firm and the vendor. A range of high-profile risk events, including large storms, have heightened the need to have up-to-date and well tested contingency plans in the event of an IT failure within the technology infrastructure. Such planning is critical to mitigate the consequences of power outages, flooding, and data redundancies. In addition to these risks, firms expressed concerns regarding resourcing, including facilities and workforce, and ensuring the availability of the requisite supporting services.

- Financial Technology Partnerships. Banking organizations have increasingly partnered with technology providers and other vendors to drive down costs (e.g., the adoption of cloud services or other IT outsourcing) or promote increased tech-enabled financial services (e.g., the growing partnership with digital lenders).

Regulatory Responses

Regulators have also been responding to these developments. Since 2008, each of the prudential banking regulators have separately issued updated guidance with respect to third-party vendor risk management. The OCC and the Federal Reserve separately issued specific guidance on third-party risk in 2013, while the FDIC issued guidance in 2008 (and proposed guidance on third-party lending in 2016 that it never finalized).[210] The Federal Financial Institutions Examination Council, an interagency group, and other agencies have also taken relevant action.[211]

Challenges Identified with the Current Approach

A number of challenges have been identified with the banking regulators' current approach to third-party vendors and service providers.

---

210. Office of the Comptroller of the Currency, Risk Management Guidance for Third Party Relationships, OCC Bulletin 2013-29 (Oct. 2013), available at: *https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html*; Office of the Comptroller of the Currency, *Supplemental Exam Procedures for Third Party Relationships, OCC Bulletin 2017-7 (Jan. 2017), available at: https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-7.html;* Office of the Comptroller of the Currency, Frequently Asked Questions to Supplement OCC Bulletin 2013-29, OCC Bulletin 2017-21 (Jun. 2017), available at: *https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-21.html*; Federal Reserve Board of Governors, Guidance on Managing Outsourcing Risk (Dec. 5, 2013), available at: *https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf*; Federal Deposit Insurance Corporation, Examination Guidance for Third-Party Lending (July 29, 2016), available at: *https://www.fdic.gov/news/news/financial/2016/fil16050a.pdf*; Federal Deposit Insurance Corporation, Third-Party Risk – Guidance for Managing Third-Party Risk, FIL-44-2008 (June 6, 2008), available at: *https://www.fdic.gov/news/news/financial/2008/fil08044.html.*

211. Karen Ross and Doug Posey, Davis Wright Tremaine LLP, *FFIEC Releases New Booklet for the Supervision of Technology Service Providers* (Nov. 19, 2012), available at: *https://www.paymentlawadvisor.com/2012/11/19/ffiec-releases-new-booklet-for-the-supervision-of-technology-service-providers/;* Brian J. Hurh, Davis Wright Tremaine LLP, *FTC Order Against Fraudulent Payment Processor Joins Growing List of Regulatory Actions Involving Third Party Service Providers* (Mar. 19, 2013), available at: *https://www.paymentlawadvisor.com/2013/03/19/ftc-order-against-fraudulent-payment-processor-joins-growing-list-of-regulatory-actions-involving-third-party-service-providers/;* Bureau of Consumer Financial Protection, *Service Providers*, Bulletin 2012-03 (April 13, 2012), available at*: https://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf* (Dodd-Frank grants the Bureau supervisory and enforcement authority over supervised service providers); Compliance Bulletin and Policy Guidance; 2016-02, Service Providers (Oct. 19, 2016) [81 Fed. Reg. 74410 (Oct. 26, 2016)].

Regulatory Efficiency and Uncertainties

Both banks and service providers have raised concerns about the growing compliance costs related to third-party oversight. Significant service providers[212] have raised concerns about inefficiencies in oversight because they are overseen by both federal banking regulators and each bank to which they provide a service. Banks of all sizes have raised concerns about the cost of compliance because multiple banks subject the same vendors to similar third-party oversight, related due diligence, and other requirements.

Banking agencies' third-party guidance, while broadly similar, is also not entirely consistent. The inconsistencies can be compounded by the inconsistent application of standards by individual examination teams within agencies. Some areas of existing guidance that firms struggle to apply uniformly may include the scope of vendors or third-parties covered, the categorization of which partners should be subject to heighted risk-based attention, and the terms and conditions that banks are expected to require of these partners. Banks have also said there is some lack of clarity in how this regulatory framework applies to data aggregators (see the discussion on clarifying when data aggregators are subject to third-party guidance in the preceding chapter on Embracing Digitization, Data, and Technology).

Related to these inconsistencies in third-party oversight, banking organizations have raised concerns about the strict implementation of such guidance through the "trickle-down" of best practices (i.e., where the most stringent due diligence standards available are expected for many vendors). While the written guidance for third-party risk generally allows for risk-based or more tailored approaches, a number of factors contribute to more stringent de facto regulation. For example, banks looking to avoid criticism from their examiners might adopt a more uniformly stringent vendor oversight approach rather than trying to convince their examiners to permit a more tailored approach to vendor oversight.

Technology Partnerships

Smaller, nonbank fintech firms and banks have raised concerns that the overall burden of the third-party supervisory regime stifles the ability of new firms to partner with banks. For example, smaller and less mature nonbank start-up firms face requirements that are inappropriately tailored, such as having to complete the same due diligence information requests required of firms with significantly greater scale or complexity. Similarly, community banks have expressed concern about their capacity to undertake the requisite due diligence and ongoing vendor management (especially with larger vendors). At the same time, fintechs and banks have said that the third-party oversight framework is critical to overseeing risks in certain bank-fintech partnership activities, such as lending.

Cloud-related service relationships also appear to face some challenges. Some banking organizations have expressed difficulties in the deployment of cloud services because of the administrative burdens of getting multiple regulators on board or unclear recognition of independent audit and certification standards. Banks have noted that fintech partnerships may also be hindered by a lack of clarity about whether a third-party vendor's sub-contractors, such as a cloud-service provider

212. FFIEC TSP Handbook, at 1.

(i.e., a fourth party), must also meet due diligence requirements. Small fintech firms often lack a realistic ability to impose any such requirements upon such fourth-party vendors.

Recommendations

Federal banking regulators should, in coordination, review current third-party guidance through a notice and comment process. U.S. banking regulators should further harmonize their guidance with a greater emphasis on (1) improving the current tailoring and scope of application of guidance upon third-party vendors to improve the efficiency of oversight and (2) enabling innovations in a safe and prudent manner. Such a review should specifically consider how to:

- Further develop the framework to regulate bank partnerships with fintech lenders to apply strong and tailored regulatory oversight while also supporting efforts by banks, particularly smaller community banks, to partner with fintechs.
- Provide greater clarity around the vendor oversight requirements for cloud service providers, including clarifying how third-party guidance should apply to a third-party's subcontractors, like cloud service providers (i.e., fourth party vendors). Further discussion of cloud services oversight is addressed in the preceding chapter on Embracing Digitization, Data, and Technology.
- Support more secure methods for consumers to access their financial data, such as through API agreements between banks and data aggregators.
- Identify common tools banks can leverage as part of due diligence efforts, such as robust independent audits, recognized certifications, and collaboration among institutions in an effort to enhance efficiencies and reduce costs.
- Maintain ongoing efforts with other federal and state regulators to identify opportunities for harmonization as appropriate.

Looking ahead and recognizing the dynamic nature of financial technology developments, the banking regulators should be prepared to flexibly adapt their third-party risk relationships framework to emerging technology developments in financial services. Moreover, banking regulators should consider how to make examiners' application of interagency guidance on third-party relationships more consistent across and within the agencies.

Banks' Innovation Investments and the Scope of Permitted Activities

The scope of permitted activities for banking organizations is generally very limited. Banks and their holding companies may only engage in activities specifically permitted by law and by their regulators. Federal banking laws that govern permissible activities, including investments in innovative financial technology partnerships, are varied and implemented through various federal and state regulators.

Banks and Savings Associations

In general, the National Bank Act establishes the scope of permissible activities for national banks, the Home Owners' Loan Act establishes the scope of permissible activities for federal savings associations, and the OCC can authorize additional permissible activities for both, in accordance

with applicable statutes.[213] The National Bank Act, in particular, allows national banks to engage in (1) the "business of banking" and (2) activities that are "incidental" to the conduct of such business.[214] The OCC has generally defined the statutory term "business of banking" dynamically over time, authorizing activities to allow national banks to keep pace with developments in the financial services marketplace and the needs of customers.[215]

The OCC, for example, recognized various financial market developments over time, including the authorization of various derivatives activities (e.g., advising, structuring and executing transactions in interest rate, equity swaps, currency, and commodity derivatives products), which enabled national banks to act as key intermediaries in the development of national and global derivatives markets to facilitate the hedging and transfer of risks. The OCC similarly recognized technology developments as it authorized various electronic, data storage and software-related activities (e.g., electronic bill payments).

The OCC has also indirectly affected the scope of permissible activities for state-chartered banks because state "wild card" laws, designed to maintain competitive parity between state banks and national banks, often grant state banks the same scope of permissible activities as has been made available to nationally chartered banks and savings associations.[216]

The Federal Deposit Insurance Act also augments permissible activities of state-chartered banks. It permits state-chartered banks to engage in certain activities permissible under state law but that are not permissible for national banks as long as the FDIC determines that "the activity would pose no significant risk" to the Deposit Insurance Fund and that the state bank meets "applicable capital standards prescribed by the appropriate Federal banking agency."[217]

Holding Companies

The Bank Holding Company Act (BHC Act) provides the statutory framework for the oversight of companies that control a bank with the aim of "protecting the safety and soundness of corporately controlled banks" and maintaining the general separation of banking and commerce.[218] As a result, the BHC Act authorizes a limited set of permissible activities for bank holding companies (BHC) and their affiliates, including (1) owning, managing, and controlling banks[219] and (2) engaging in activities that are "so closely related to banking as to be a proper incident thereto" (i.e., Section 4(c)(8) authorities).[220] BHCs that apply to become and qualify as a financial holding company

213. Office of the Comptroller of the Currency, *Activities Permissible for National Banks and Federal Savings Associations, Cumulative* (Oct. 2017), at 1, available at: *https://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-other-activities-permissible-october-2017.pdf* ("OCC Cumulative").

214. 12 U.S.C. § 24 (Seventh).

215. OCC Cumulative, at 1 ("[t]he business of banking is an evolving concept and the permissible activities of national banks similarly evolve over time").

216. Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, *Report to the Congress and the Financial Stability Oversight Council Pursuant to Section 620 of the Dodd-Frank Act* (Sept. 2016), at 51, available at: *https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20160908a1.pdf* ("Section 620 Report").

217. 12 U.S.C. § 1831a(a)(1).

218. Section 620 Report, at 3.

219. 12 U.S.C. § 1843(a).

220. See 12 U.S.C. § 1843(c)(8).

benefit from a greater range of permissible activity under amendments made by the GLBA. The BHC Act, as amended by the GLBA, authorizes financial holding companies to engage in any activity that (i) the Federal Reserve, in consultation with the Secretary of the Treasury, determines is "financial in nature or incidental to such financial activity," or (2) the Federal Reserve determines is "complementary to a financial activity and does not pose a substantial risk to the safety and soundness of depository institutions or the financial system generally."[221] The BHC Act's definition of "control" is critical to determining how the statute is applied and to which firms its activity restrictions apply. The BHC Act defines "bank holding company" as any company that controls a BHC or bank (not including Industrial Loan Companies).[222] A company generally controls a BHC or bank if the company: (1) owns more than 25% of any class of voting securities; (2) controls in any manner the election of a majority of the directors of the BHC or bank; or (3) exercises "a controlling influence" over the management or policies of the BHC or bank.[223] The Federal Reserve is responsible for determining what constitutes a "controlling influence."

Figure 9: Overview of Authorities for Permitted Activities for Banking Organizations

Authorizing Federal Statute	Types of Permitted Activities	Interpreted by	Banking Organizations Subject to These Authorities
National Bank Act	Business of Banking	OCC	National Banks
	Incidental to the Business of Banking	OCC	National Banks
Federal Deposit Insurance Act	State-authorized activities that do not present risks to the Deposit Insurance Fund	State Regulators; FDIC	State-chartered Banks
Bank Holding Company Act (as amended by GLBA)	Managing and controlling an insured depository	Fed	All Bank Holding and Financial Holding Companies
	Closely related to banking or an incident thereto	Fed	All Bank Holding and Financial Holding Companies
	Financial in nature or incidental to a financial activity (e.g., securities and insurance)	Fed; Treasury	Financial Holding Companies
	Complementary to a financial activity and that does not present risks to inst. safety or the financial system generally	Fed	Financial Holding Companies

Source: National Bank Act, 12 U.S.C. §§ 24 and 24a; Federal Deposit Insurance Act, 12 U.S.C. § 1831a; Bank Holding Company Act, 12 U.S.C. § 1843. The permissible activities available to state-chartered banks is also determined by National Bank Act authorities because states have adopted laws that generally maintain parity with national banks' scope of permitted activities.

221. 12 U.S.C. § 1843(k)(1); see also Section 620 Report, at 4-5.

222. 12 U.S.C. § 1841(a)(1).

223. 12 U.S.C. § 1841(a)(2).

Challenges with the Current Approach

The restrictions on BHCs' permissible activities and investments present several interrelated challenges to innovation efforts by these firms.

Responding to market developments, BHCs have sought to invest in various financial technology-related firms to facilitate innovation. However, the current application of the BHC definition of "control" can discourage banks from such investments, because (1) fintech firms receiving BHC investments would like to avoid being considered a BHC affiliate because they would become subject to BHC-related regulations, including becoming subject to the applicable activities restrictions (discussed above); and (2) "control" can be difficult to determine because it relies upon Federal Reserve discretion under a process that is not sufficiently transparent. One of the considerations for defining "control" is the nature of the business relationship between the BHC and the firm receiving the equity investment. A BHC may seek to expand its business relationship with a successful fintech in which it has invested, yet doing so could then trigger "control" and the attendant BHC Act regulatory requirements.

More generally, banking organizations are increasingly required to deploy new technologies to serve customer needs and may do so through acquisitions, partnerships, or internal development. In particular, the highly dynamic nature of financial technologies today could result in banking regulators considering certain technology-based business activities impermissible or disagreeing on whether such an activity is permitted under each regulator's respective statutory authority.

Recommendations

To support the ability of firms to flexibly adapt to new technology and market developments, Treasury recommends that the Federal Reserve consider how to reassess the definition of BHC control to provide firms a simpler and more transparent standard to facilitate innovation-related investments. This recommendation is consistent with public comments by Federal Reserve officials who have called for reassessing this issue. In addition, the banking regulators should interpret banking organizations' permitted scope of activities in a harmonized manner as permitted by law wherever possible and in a manner that recognizes the positive impact that changes in technology and data can have in the delivery of financial services.

Updating Activity-Specific Regulations

Overview

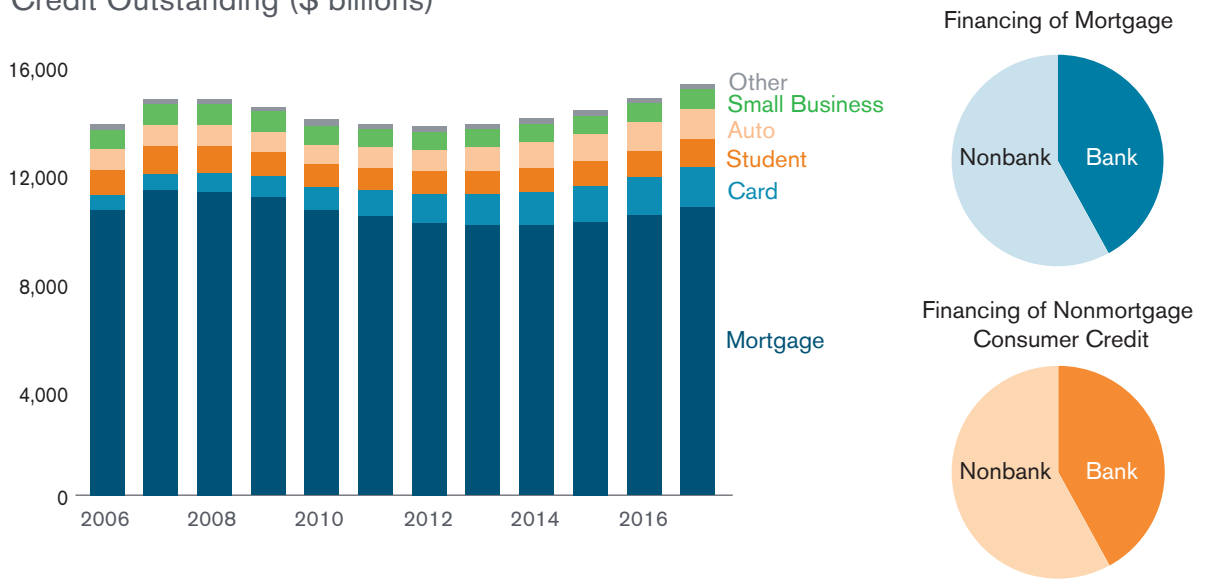
The U.S. regulatory framework for key financial service activities — lending, payments, and financial planning — requires meaningful reform to better enable the delivery of both digital and nondigital financial services to consumers and businesses. This chapter discusses these regulatory challenges and also identifies a number of specific recommendations aimed at improving the U.S. regulatory approach to lending, payments, and financial planning.

Lending and Servicing

Household and Small Business Lending

U.S. households and small businesses derive credit from a highly diverse mix of banks and nonbank firms. These firms provide secured and unsecured financing to their clients and perform a range of activities fulfilling that mission, including loan sourcing and origination, credit underwriting, and loan servicing. Although banks and nonbanks access securitization markets to monetize, through sale, pools of loans that they originate, the two sectors are generally differentiated by the ability to retain loans in portfolio. Banks are able to use deposit funding to reliably retain loans over their life in portfolio. By comparison, nonbanks generally have relatively limited balance sheet capacity that is provided by their equity capital and a combination of long-term debt and short-term secured borrowing. As such, they often take an approach that is typically referred to as an "originate to distribute" business model.

Figure 10: Mortgage, Consumer, and Small Business Credit Outstanding ($ billions)



Source: Federal Reserve Financial Accounts of the United States and Keith Horowitz and Jill Shea, Citi Research, *U.S. Banks and Credit Cards* (May 2018).
Data as of Q4 2017. "Bank" denotes holdings by U.S.-chartered financial institutions.

Outstanding credit to households and small businesses exceeded $15 trillion in 2017, of which residential mortgages accounted for $10.6 trillion, cards and revolving credit accounted for $1 trillion, student credit accounted for $1.5 trillion, auto lending $1.1 trillion, and small business lending $700 billion. As shown in **Figure 10**, nonbank firms constitute a significant share of the overall funding provided across these lending segments. For example, nonbank companies account for 58% of the outstanding non-mortgage consumer loan market and 58% of the total residential mortgage market as of the first quarter of 2018.[224]

The share of nonbank lending in the U.S. residential mortgage market has been significant in recent decades due in part to the availability of warehouse financing and access to federally supported securitization programs for both private and government-supported loan programs, as conducted by Fannie Mae and Freddie Mac (the government-sponsored enterprises, or GSEs) and Ginnie Mae.[225] Of the $1.8 trillion of mortgage originations in 2017, approximately 30% were retained in portfolio (generally by the originator).[226] Except for a relatively limited amount of issuance through private-label securities (PLS), most of the remaining 70% of 2017 volume was securitized by the GSEs or Ginnie Mae.[227] Nonbanks enjoy access to these securitization channels on largely equal footing to banks, which supports their ability to accommodate a large share of the origination market.

As discussed later in this chapter, the value proposition of marketplace lenders has resulted in their expansion, though these firms account for just a small fraction[228] of the much larger, multi-trillion dollar consumer credit market. Installment and payday lending activity have consistently been dominated by nonbanks, though banks and credit unions have historically provided some products that served similar short-term, small-dollar financing needs.

The U.S. capital markets are the largest, deepest, and most vibrant in the world. The nation's economy successfully derives a larger portion of business and consumer financing from its capital markets, rather than the banking system, than most other advanced economies. This includes reliable access to capital through securitization, a capital market evolution that has consistently been enabled by advances in information technology and the increased scope and cost-effectiveness of data storage and data management.

---

224. Keith Horowitz and Jill Shea, *Citi Research: U.S. Banks and Credit Cards* (May 2018).

225. For a discussion of how the rise of the secondary mortgage market and new federal regulation were contributors to a more unbundled housing finance system, see James R. Follain and Peter M. Zorn, *The Unbundling of Residential Mortgage Finance*, 1 J. of Housing Res. 63 (1990), available at: *https://www.innovations.harvard.edu/sites/default/files/jhr_0101_follain.pdf*.

226. Treasury analysis based on data from Fannie Mae, Freddie Mac, the U.S. Department of Housing and Urban Development (HUD), and the U.S. Department of Veterans Affairs (VA).

227. Id.

228. Hannah Levitt, *Personal Loans Surge to a Record High*, Bloomberg (July 3, 2018), available at: *https://www.bloomberg.com/news/articles/2018-07-03/personal-loans-surge-to-a-record-as-fintech-firms-lead-the-way* (analyzing data from TransUnion).

Emerging Digitization of Lending

Technological changes, including digitization, help drive changes to the lending landscape. Digital lending is increasingly prevalent throughout the household and small business lending market.

Nonbank digital lenders have gained outsized attention in recent years, driven in part by their rapid rate of growth and employment of new technology-intensive approaches to lending. These firms, such as marketplace lenders active in consumer and small business lending, have digitized the customer acquisition, origination, underwriting, and servicing processes. Moreover, these lenders are designing these digital services to provide customer experiences that are seamless and more timely than the techniques generally employed by traditional lenders. These changes also appear to reduce expenses, which lowers the cost of credit as well as providing greater access to credit.

In contrast, many financial institutions have yet to digitize their lending at a similar level.[229] For example, many banks have yet to fully digitize their origination processes. Banks report that less than half have digitized some aspects of their loan origination channels.[230] Moreover, the degree of digitization is much less comprehensive than new digital lenders. Even for banks that offer a digital origination channel, one industry survey found that the online features may vary, as 90% or more have digitized the application processes, but less than half provide for electronic signatures and document uploads, only a third provide online customer service, and less than 20% provide instant credit decisions.[231]

Key elements of digitization employed by new digital lenders are rapidly expanding across the wider banking and financial institution landscape and are expected to permeate all major lending segments over time. Within the mortgage industry, for example, Federal Reserve Bank of New York research staff estimates that stand-alone nonbank mortgage originators that offer a mortgage application process entirely online have expanded from 2% of the market in 2010 to 8% of the market in 2016.[232] Moreover, the partnerships between banks and new digital lenders have been expanding and are poised to increase over time, potentially serving to narrow the gap in practices between those two sectors for the benefit of both consumer and business segments.

Regulatory Landscape

Lending is a highly regulated activity that is overseen by a large number of federal and state authorities in the United States.

Federal laws and regulations are extensive and cover fair credit reporting, fair debt collection, fair lending, credit practices, fair credit billing, consumer privacy, electronic signature, and electronic

---

229. See American Bankers Association, *The State of Digital Lending* (Jan. 2018), at 4-7, available at: *https://www.aba.com/Products/Endorsed/Documents/ABADigitalLending-Report.pdf* ("Traditional banks, particularly smaller ones, have typically lagged in technology adoption for lending, especially compared to up-and-coming fintech players"). Factors such as regulatory complexity and burdens, technology budgets, or third-party service provider reliance may contribute to the slow adoption of digitized lending by these institutions.

230. Id.

231. Id. at 9.

232. Andreas Fuster et al., *The Role of Technology in Mortgage Lending*, Federal Reserve Bank of New York Staff Report No. 836 (Feb. 2018), available at: *https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr836.pdf*.

transfer of funds, among others. Appropriately, there is a wide range of rules, such as consumer laws governing credit card issuers, mortgage lending and servicing, and automobile financing. At the federal level, the Bureau of Consumer Financial Protection (the Bureau) has authority to implement many federal statutes affecting consumers, in addition to requirements imposed by prudential regulators, namely the Board of Governors of the Federal Reserve System, OCC, FDIC, and National Credit Union Administration (NCUA). This multiplicity of regulatory authority is itself an outcome of a fragmented regulatory environment that at times can lead to overlap, duplication, and uncertainty.[233]

At the state level, there are licensing or registration requirements to operate within a state, state-specific maximum rates of interest on debt, state-specific loan value caps, and other consumer protections. State requirements are largely enforced by state financial regulatory authorities and state attorneys general.

Both federal and state regulators also have enforcement authorities that generally include authorities to prevent consumer financial service providers from engaging in unfair, deceptive, or abusive acts or practices.[234]

Marketplace Lending

Overview

A number of digitally focused lenders, often referred to as marketplace lenders or "fintech lenders," have recently emerged and grown rapidly. Fintech lenders represented 36% of the unsecured consumer loan market in 2017[235] and around 2% of the small business market in 2014,[236] but in both instances are experiencing rapid rates of growth and market penetration. Marketplace lenders have generated significant attention due to many of the underlying features of these new lending models. Notable characteristics of the sector include newly branded firm and product launches; lack of reliance on brick-and-mortar branches for delivery of services; leverage of innovative technological approaches in marketing, sourcing, and fulfilling loan demand; and extensive use of data and data management techniques in credit underwriting processes.

Marketplace lenders operate with a diversity of business models that can generally be characterized by the asset classes and customer segments that they serve, the manner in which they access the national market, and their funding and risk-management strategies.

---

233. The FTC maintains some residual consumer protection authority over nonbank entities.

234. Dodd-Frank granted authority for the Bureau to bring enforcement actions against certain consumer financial service providers for "unfair, deceptive, or abusive" acts. See Dodd-Frank § 1031(a) [12 U.S.C.§ 5531(a)]; see also Richard E. Gottlieb, Arthur B. Axelson, and Thomas M. Hanson, *Consumer Financial Services Answer Book*, Practising Law Institute (2016); American Bankers Association, *Consumer Lending, Seventh Edition* (2013) (discussing consumer laws impacting banking organizations).

235. Hannah Levitt, *Personal Loans Surge to a Record High*, Bloomberg (July 3, 2018), available at: *https://www.bloomberg.com/news/articles/2018-07-03/personal-loans-surge-to-a-record-as-fintech-firms-lead-the-way* (analyzing data from TransUnion).

236. Karen Gordon Mills and Brayden McCarthy, *The State of Small Business Lending: Innovation and Technology and the Implications for Regulation*, Harvard Business School Working Paper 17-042 (2016), at 48, available at: *https://www.hbs.edu/faculty/Publication%20Files/17-042_30393d52-3c61-41cb-a78a-ebbe3e040e55.pdf*.

Target Product Segments

The focus of marketplace lenders has primarily been the provision of unsecured credit to individuals (primarily utilized for the purpose of debt consolidation) and working capital to small businesses. However, business models are constantly evolving, and firms are beginning to expand into other product segments.

- Unsecured Consumer. Consumers access unsecured credit to pay down credit card or other debt, finance an online purchase, or manage variable expenses. A typical unsecured consumer loan in this market has a balance of $14,000, an annual interest rate of 14.7%, and a 4-year term.[237]
- Small-Dollar Consumer Lending. A subset of unsecured consumer lenders focus on loans with shorter terms and higher interest rates that typically exceed a 36% annual percentage rate (APR), which is a widely used rate cap.[238] These loans typically have lower balances, below-average credit characteristics, and can be viewed as an alternative to other forms of lending, such as payday lending. These products serve a unique niche of consumers that may not have many alternatives to high-priced credit.
- Student. Student lenders primarily focus on refinancing traditional federal and private student loan debt with unsecured installment debt, generally focused on borrowers with prime FICO scores and several years of employment history who can qualify for lower rates (generally ranging from 3-7%).
- Small Business. Small business loans are typically less than $500,000, with APRs that may average 7-48% and terms that range from six months to three years. [239]
- Auto Finance. This segment focuses on the $1.1 trillion auto loan industry, which accounts for approximately 30% of nonmortgage consumer debt, and has been facilitated by the trend of migration of financing away from captive finance subsidiaries of manufacturers.[240]

National Lending Business Model Strategies

Marketplace lenders currently lend to customers across the country through two primary models: (a) a bank partnership model in which a bank originates the loan, which is generally sourced and serviced by the marketplace lender and funded in a variety of manners; and (b) a direct lender model in which the marketplace lender acquires the applicable regulatory licenses in each U.S.

---

237. Testimony of Nathaniel L. Hoopes, Marketplace Lending Association, before the House Financial Services Committee (Jan. 30, 2018), at 3-4, available at: *https://financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-nhoopes-20180130.pdf*.

238. The 36% rate cap for low-balance consumer lending emerged in the first half of the twentieth century in the United States and still exists today as a statutory maximum in many states. For additional information, see Lauren K. Saunders, National Consumer Law Center, *Why 36%? The History, Use, and Purpose of the 36% Rate Cap* (Apr. 2013), available at: *https://www.nclc.org/images/pdf/pr-reports/why36pct.pdf*.

239. S&P Global Market Intelligence, *2017 U.S. Digital Lending Landscape*, at 5-6 and company disclosures from Credibly, Kabbage, and OnDeck.

240. Financial Technology Partners, *Auto Fintech – The Emerging Fintech Ecosystem Surrounding the Auto Industry* (Dec. 2017), available at *https://www.ftpartners.com/fintech-research/auto-fintech*.

state in which it intends to do business. Under the bank partnership model, where, for example, a bank originates a loan and contracts with a marketplace lender to service the loan for the bank, federal law allows the bank, and federal jurisprudence allows the marketplace lender servicing the loan, to charge interest at the rate allowed by the laws of the state where the bank is located, even if the rate is higher than the rate allowed under the laws of the state where the loan is made.[241] Firms whose target loan products are at less of a risk of exceeding state usury limits, such as high-quality unsecured consumer installment loans, may find the direct licensing model relatively attractive.

Other Business Model Features

Firms are differentiating themselves along other key dimensions from those cited earlier, including:

- Credit Risk. The predominant business model for marketplace lenders is an "originate to distribute" approach where there is limited long-term balance sheet retention of loans that they originate. This is similar to the business model of many traditional nonbank finance companies, such as independent mortgage bankers, that have consistently relied on securitization to fund their loan production. Most lenders, however, will retain servicing obligations on the outstanding loans — collecting payments from borrowers, remitting payments to creditors, and handling loss mitigation. Some firms may participate in the ongoing credit risk exposure by retaining a share of loans (or some proportional share of credit risk). This can arise from Dodd-Frank risk-retention requirements[242] or to better align interests with investing partners through a "skin-in-the-game" approach.
- Funding Strategy. Initially, marketplace lenders adopted a "peer-to-peer" funding model where individual loans were funded on digital platforms with individual investors, or "peers," providing the majority of the capital. However, these distribution methods have evolved and now include a wide variety of both retail and institutional sources. While some firms have publicly traded equity, many are privately held. Marketplace lenders have a range of funding structures with a diverse set of investors such as banks, traditional asset managers, hedge funds, family offices, and high net worth individuals.
- Credit Underwriting Models. Nearly all marketplace lenders are built around online digital platforms designed to deliver rapid credit decisions. Some firms report the use of advanced analytical tools, such as machine learning, and various data sources such as bank transaction data, which includes real-time data linked from borrower accounts, model-based income estimates, and social media. An important element of underwriting for marketplace lenders is their use of aggregated data from third-party firms. Finally, many of the firms have departed from the strict use of credit ratings in favor of more data-driven techniques to drive their credit decision-making.

Industry Growth

The growth of marketplace lending volumes and the corresponding securitization market has been on a strong upward trajectory since at least 2013. Estimates for cumulative loans originated since

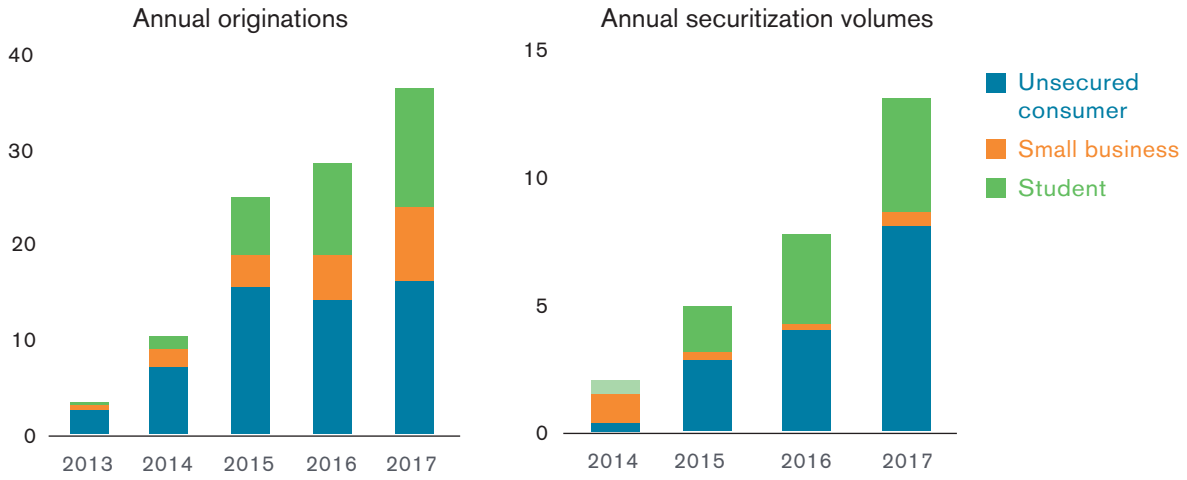
241. See 12 U.S.C. § 85; *Madden v. Midland Funding, LLC*, 786 F.3d 246, 250-253 (2d Cir. 2015), cert. denied, 136 S. Ct. 2505 (2016).

242. See 15 U.S.C. § 78o-11.

2014 total almost $100 billion, according to industry data sources.[243] Of this amount, unsecured consumer lending is the largest category, amounting to about 50% of the total.[244] The securitization market for loans originated by marketplace lenders has similarly remained robust since securitization of this type of credit began to scale up in 2013.

In the first half of 2016, questions about the fragility of the funding model and the potential for conflicts of interest between investors and marketplace lenders led to a brief downturn in industry volumes. Since then, firms within the industry have worked to improve standards for their business models. In addition, better relationships with investors have allowed for concerns related to how loan characteristics are disclosed and how loans are allocated to investors to be addressed.

Figure 11: Market Growth of Marketplace Lending ($ billions)



Source: S&P Global Market Intelligence for originations and PeerIQ for securitisation volumes. Each methodology is based on a different subset of marketplace lenders.

Access to Credit

Early evidence indicates that these new lending channels have provided opportunities to expand credit to underserved segments. For example, a July 2017 study[245] found that new marketplace lenders have tended to expand credit in areas where bank branches have been on the decline. Moreover, this same study found that borrowers with similar credit risk profiles could obtain more favorably priced credit than alternatives such as credit cards. The study also found some evidence that the use of alternative credit data in this space allowed consumers with weaker traditional credit profiles to access credit. This study used data from the largest marketplace lender, Lending Club, and covered loans originated between 2007 and 2016.

243. S&P Global Market Intelligence, *2017 U.S. Digital Lending Landscape*.

244. Id.

245. Julapa Jagtiani and Catharine Lemieux, *Fintech Lending: Financial Inclusion, Risk Pricing, and Alternative Information*, Federal Reserve Bank of Philadelphia Working Paper 17-17 (2017), at 9-12, available at: *https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2017/wp17-17.pdf*.

The conclusions of this study, while preliminary, are not entirely unexpected given that the primary purpose of many marketplace loans is to refinance higher rate debt into less expensive debt. A number of marketplace lenders are specifically aiming to build underwriting models designed to achieve better results through providing lower priced credit for a given traditional FICO score. However, with only a few years of credit performance, these credit models have yet to be tested in various macroeconomic environments that would include either higher interest rates or a general economic downturn. Traditional financial institutions, including banks, have also begun sourcing deposits and extending credit through technology-enabled web platforms instead of utilizing their traditional brick-and-mortar footprint.

Regulation and Supervision of Marketplace Lenders

Marketplace lenders may be supervised or overseen by federal and state agencies, directly or indirectly, depending on whether they utilize the bank partnership model or the direct lending model. Under the direct lending model, marketplace lenders must have licenses in most states where they do business and are subject to oversight in those states. Marketplace lenders that partner with banks may be subject to regulation and examination by federal banking regulators because they may be considered third-party service providers to a regulated banking entity[246] and by virtue of guidance pertaining to vendor management. Marketplace lenders that use the bank partnership model may remain subject to various state requirements, depending on the approaches used by state regulators.

All lenders, including banks and marketplace lenders, are subject to federal regulation in areas such as consumer protection, anti-money laundering, and securitization.

- Consumer Protections: For consumer lenders, a number of federal and state consumer protection requirements may apply, including the Truth in Lending Act, anti-discrimination requirements under the Equal Credit Opportunity Act, and provisions governing electronic transfers under the Electronic Funds Transfer Act. Marketplace lenders may also be subject to regulation under the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and other laws.
- Anti-Money Laundering: Marketplace lenders may have legal obligations to comply with the Bank Secrecy Act (BSA).
- Securitization: To the extent that marketplace lenders engage in securitization and offer those securities to the public, they may be subject to requirements under the Securities Act of 1933. These marketplace lenders must register the securities with the SEC, unless an exemption applies, and may be subject to risk-retention requirements.

Marketplace lenders, however, are not subject to numerous regulations that apply to banks, ranging from Community Reinvestment Act (CRA) requirements to prudential standards such as capital and liquidity requirements, deposit insurance requirements and assessments, resolution-planning requirements, and prompt corrective action requirements. These differences in regulation illustrate the challenge in determining an appropriate regulatory environment across providers of financial services.

246. See 12 U.S.C. § 1867(c)(1).

Issues and Recommendations

Key Considerations for the Bank Partnership Model

Some state regulators and consumer groups have expressed concern that the bank partnership model can harm consumers by allowing partnering firms to bypass state-based usury limits and other state requirements. Advocates note that some lenders operate with high-APR business models and offer loans whose APRs can exceed 100%, when fees are included.[247] Beyond enabling high-APR products, advocates note that in the past, such third-party partnerships have enabled some deceptive practices.[248]

Today's marketplace lenders, however, generally compete on the basis of providing a more affordable cost of credit (e.g., refinancing credit card and other debts) and an enhanced consumer experience. Many of these consumer-facing lenders generally operate below a 36% APR threshold and have stated that they would welcome a 36% APR cap for consumer lending, including loans originated through bank partnership arrangements.[249] Federal banking regulators are also paying closer attention to third-party service provider relationships, specifically lending arrangements, which should reduce the risk of potential abuse witnessed in past partnership arrangements.

Concerns about potentially harmful consumer lending practices also need to be considered against the possible benefits that such bank partnership relationships can provide to underserved borrower segments. Traditional lenders often provide lending experiences that are slower (e.g., because of extended wait times for credit decisions) and difficult due to cumbersome application and fulfilling processes. Many lenders may also not adequately serve certain lending segments, like smaller-balance, small business, or unsecured consumer borrowers with less-established credit histories.

Appropriately designed lending partnerships can leverage advantages from both banks and fintechs to improve upon the currently provided products. A recent study stated that 71% of banks were interested in partnering with a third-party digital platform for consumer loan origination and nearly 80% of banks were interested in using technology to support their small business lending.[250] For example, in the small-dollar lending segment, there appears to be market demand for banks to engage further in these markets[251], as their cost of capital could be used to deliver products that are very competitive with rates charged by nonbank payday lenders.

---

247. Letter from the National Consumer Law Center et al. to the Federal Deposit Insurance Corporation, *Re: Comments on Proposed Financial Institutions Letter (FIL) 50-2106: Third-Party Lending* (May 2017), available at: *https://www.nclc.org/images/pdf/rulemaking/comments-fdic-3rdparty-lending.pdf*.

248. For example, the OCC took action in 2003 to address deceptive credit card programs marketed through a third-party vendor. Office of the Comptroller of the Currency, *News Release – OCC Concludes Case Against First National Bank in Brookings Involving Payday Lending, Unsafe Merchant Processing, and Deceptive Marketing of Credit Cards* (Jan. 21, 2003), available at: *https://www.occ.treas.gov/news-issuances/news-releases/2003/nr-occ-2003-3.html*.

249. Marketplace Lending Association, *Submission to the U.S. Department of the Treasury* (May 2018).

250. American Bankers Association, *The State of Digital Lending* (Jan. 2018), available at: *https://www.aba.com/Products/Endorsed/Documents/ABADigitalLending-Report.pdf*.

251. Pew Charitable Trusts, *Americans Want Payday Loan Reform, Support Lower-Cost Bank Loans* (Apr. 2017), available at: *http://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2017/04/americans-want-payday-loan-reform-support-lower-cost-bank-loans*.

Treasury recognizes that these existing bank partnership arrangements have generally enhanced the provision of credit to consumers and small businesses. Treasury makes the following specific recommendations to address constraints that would unnecessarily limit the prudent operation of partnerships between banks and marketplace lenders.

Valid-When-Made/Madden v. Midland

Several legal issues have presented risks to the bank partnership model used by marketplace lenders. Specifically, in *Madden v. Midland Funding, LLC*, the Second Circuit held, in part, that the National Bank Act (NBA), which preempts state usury laws with respect to the interest a national bank may charge on a loan, did not preempt state-law usury claims against a third-party debt collector that had purchased the loan.[252] In its ruling, the court did not refer to the "valid when made" common law doctrine, which provides that a loan contract that is valid when it was made cannot be invalidated by any subsequent transfer to a third party. In an amicus brief at the certiorari stage, the United States took the view that the court of appeals "erred in holding that state usury laws may validly prohibit a national bank's assignee from enforcing the interest-rate term of a debt agreement that was valid" when made under the applicable state law.[253] The Supreme Court declined to hear the case.

Because of *Madden*, the ability of nondepository third parties (e.g., marketplace lenders) to collect debts originated by depository institutions in reliance upon federal preemption of state usury law limits could be limited in the Second Circuit, ultimately restricting access to credit. In particular, unsecured consumer credit could be diminished because nonbank firms such as marketplace lenders may be discouraged from purchasing and attempting to collect on, sell, or securitize loans made in these states because of the risk of litigation asserting violations of state usury laws. One study of the impact of the *Madden* decision showed an observable relative decline in the growth of such loans in two states within the jurisdiction of the Second Circuit (New York and Connecticut),[254] compared to loans originated outside the Second Circuit.[255] If adopted more broadly, the rule announced in *Madden* could have broader implications well beyond marketplace lenders. Other credit markets that could be affected include bank/loan intermediary partnerships, debt collection activities, loan securitization activities, and simple loan transfers.[256] In response to *Madden*, some lenders are changing their lending and securitization activities by, for example, excluding loans from Second Circuit states in their pools altogether.[257]

---

252. See *Madden*, 786 F.3d at 249-53.

253. Am. Brief of the United States, *Midland Funding, LLC*, No. 15-610 (2016) (opposing certiorari). Although the United States argued that the Second Circuit erred, the government recommended that the petition for certiorari should be denied due to lack of a circuit split.

254. The Second Circuit encompasses New York, Vermont, and Connecticut.

255. Colleen Honigsberg, Robert J. Jackson, Jr., and Richard Squire, *How Does Legal Enforceability Affect Consumer Lending? Evidence from a Natural Experiment*, 60 J. L. & Econ. 673 (Nov. 2017).

256. *The Curious Case of* Madden v. Midland Funding *and the Survival of the Valid-When-Made Doctrine*, The Free Library. 21 N.C. Banking Inst. 1 (2017).

257. Honigsberg, Jackson, and Squire.

Recommendations

Treasury recommends that Congress codify the "valid when made" doctrine to preserve the functioning of U.S. credit markets and the longstanding ability of banks and other financial institutions, including marketplace lenders, to buy and sell validly made loans without the risk of coming into conflict with state interest-rate limits. Additionally, the federal banking regulators should use their available authorities to address challenges posed by *Madden*.

True Lender

Recent court decisions have exposed bank partnership models to uncertainty regarding whether the bank or nonbank partner is the "true lender" in providing credit.[258] Some of these decisions have deemed the nonbank partner as the true lender,[259] which subjects the nonbank partner to a range of state-based requirements including interest rate limits and licensing requirements.

The result of these decisions is a variety of standards for determining which entity is the true lender, leading to market uncertainties that harm the viability of the bank partnership model. For example, one court applied a "predominant economic interest" standard, under which the court analyzed the "totality of the circumstances to determine which entity had the predominant economic interest" in the loan.[260] However, compliance with such a standard on an ex-ante basis could be difficult because of nuances in how a court might determine the predominant economic interest. Firms enter into partnership arrangements in which they negotiate a range of terms and conditions based upon a variety of market, economic, and other considerations. The uncertainties created by these court cases create pressure to alter these partnership arrangements based upon nonmarket factors. Some marketplace lenders, for example, have already restructured their economic relationships with partnering banks to better account for the risks presented by these court cases. A fragmented legal structure creates an inefficient regulatory framework and significant compliance challenges for the bank partnership model.

FDIC's Proposed Third-Party Lending Guidance

The FDIC published a letter on July 29, 2016, seeking comment on proposed guidance on third-party lending,[261] which was generally regarded as a response to the rise of online marketplace lenders establishing "bank partnership" funding models.

The proposed guidance would supplement and expand upon the principles outlined in the FDIC's existing guidance for managing third-party risk by establishing specific expectations

258. See, e.g., *CashCall, Inc. v. Morrisey*, No. 12-1274, 2014 W. Va. LEXIS 587, at *39-44 (W. Va. May 30, 2014).

259. See id.

260. See id.

261. Federal Deposit Insurance Corporation, *FDIC Seeking Comment on Proposed Guidance for Third-Party Lending*, FIL-50-2016 (July 29, 2016), available at: *https://www.fdic.gov/news/news/financial/2016/fil16050.html*. Financial Institution Letter 50-2016 is an unfinished proposal on third party lending from the FDIC.

for third-party lending arrangements.[262] For FDIC-supervised institutions that engage in significant lending activities through third parties, the proposal suggested increased supervisory attention, including a 12-month examination cycle, concurrent risk management and consumer protection examinations, offsite monitoring, and possible review of third parties on an ongoing basis.

Many marketplace lenders welcomed the FDIC's proposed guidance, as it would help affirm the validity of such bank partnerships by providing some federal supervision. Smaller banks note that such third-party lending guidance could also improve their ability to partner with fintech lenders. Banks more generally have raised concerns with the proposed guidance, such as with (1) the breadth of the proposed definitions of third-party lending, and (2) the potential for inconsistencies between banks where FDIC is the primary federal regulator and other types of banks because the FDIC would be the only regulator issuing such guidance.[263]

Recommendations

Treasury recommends that Congress codify that the existence of a service or economic relationship between a bank and a third party (including financial technology companies) does not affect the role of the bank as the true lender of loans it makes. Further, federal banking regulators should also reaffirm (through additional clarification of applicable compliance and risk-management requirements, for example) that the bank remains the true lender under such partnership arrangements.

Credit Services

An area of growing legal complexity for the bank partnership model is the provision of additional credit services. Some states apply licensing obligations to parties that are offering to arrange bank loans. In *CashCall, Inc. v. Maryland Commissioner of Financial Regulation*, the Maryland Court of Appeals ruled that CashCall, a payday loan broker, could not offer to arrange loans for Maryland residents for a fee without obtaining a license under the Maryland Credit Services Business Act (MCSBA).[264] In addition to requiring a license, the MCSBA prohibits a credit service business from assisting a consumer in obtaining a loan that exceeds the state's usury rate.[265] The MCSBA defines a "credit services business" to include any entity that obtains or assists a consumer in obtaining an extension of credit "in return for the payment of money or other valuable consideration,"[266] which the court interpreted to apply to the nonbank[267] In a similar case in West Virginia, an online marketplace

262. The proposed guidance defines third-party lending as "a lending arrangement that relies on a third party to perform a significant aspect of the lending process." This is likely to include relationships with many online marketplace lenders. Further, the proposed guidance defines "significant" third-party lending arrangements as those, for example, that have a material impact on revenues, expenses, or capital; involve large lending volumes in relation to the bank's balance sheet; involve multiple third parties; or present material risk of consumer harm.

263. American Bankers Association, *Comment Letter Re: FIL-50-2016: FDIC Seeking Comment on Proposed Guidance for Third-Party Lending* (Oct. 26, 2016), available at: *https://www.aba.com/Advocacy/commentletters/Documents/ABACommentLetterFDICProposedThirdPartyLendingGuidance.pdf*.

264. *CashCall, Inc. v. Maryland Commissioner of Financial Regulation*, 139 A.3d 990, 1004-06 (Md. 2016).

265. Md. Code Com. Law § 14-1902(9).

266. Md. Code Com. Law § 14-1901(e).

267. *CashCall*, 139 A.3d at 1000.

lender entered into a settlement agreement with the West Virginia Attorney General for failing to obtain a credit service license and charging rates higher than permitted under state law.[268]

Since more than three-quarters of the states have a credit services organization law, these cases create legal uncertainty for the bank partnership model.[269] Instead of focusing on whether the nonbank is the true lender or whether the loan was valid when made by the bank, these cases inhibit the ability of the nonbank to partner with a bank.

Recommendations

Treasury recognizes the role of state laws and oversight in protecting consumers, but such state regulation should not occur in a manner that hinders bank partnership models already operating in a safe and sound manner with appropriate consumer protections. Treasury recommends that states revise credit services laws to exclude businesses that solicit, market, or originate loans on behalf of a federal depository institution pursuant to a partnership agreement.

Mortgage Lending and Servicing

Overview

In the Banking Report, Treasury highlighted the steep increases in the cost to originate and service a mortgage loan as evidence of the burden of post-crisis mortgage regulation.[270] Treasury found that new regulations, combined with the use of enforcement actions, were effectively imposing a regulatory tax on the mortgage marketplace by requiring lenders to hold additional liability reserves and add compliance personnel, if not exit certain markets altogether. In response, Treasury offered recommendations to recalibrate and clarify rules where they were unnecessarily raising the cost and restricting access to mortgage credit.[271]

Concurrent with, and partially driven by, the introduction of the post-crisis regulatory regime, the primary mortgage market experienced a fundamental shift in composition and concentration. Traditional, deposit-based lender-servicers have ceded significant market share to specialty, nondepository mortgage lender-servicers, often referred to as nonbanks or independent mortgage banks, that are licensed and regulated for safety and soundness at the state level. In 2007, these mortgage banks originated just over 20% of all new single-family, first-lien mortgages and comprised 4 of the top 20 lenders.[272] By 2016, nondepository lenders accounted for just under half of new loans and 12 of the top 20 lenders.[273]

---

268. Chris Dickerson, *Morrisey's Office Reaches $336K Settlement with Avant Online Lender*, W.V. Record (June 6, 2016), available at: *https://wvrecord.com/stories/510785558-morrisey-s-office-reaches-336k-settlement-with-avant-online-lender*.
269. Mike Whalen, Goodwin Procter LLP, *Bank Partnership Or Go It Alone?* (Aug. 23, 2016), available at: *https://www.goodwinlaw.com/publications/2016/08/08_23_16-bank-partnership-or-go-it-alone*.
270. The Banking Report, at 92-102.
271. Id.
272. SNL and Home Mortgage Disclosure Act (HMDA) data.
273. Id.

The growth of nonbank mortgage lenders and servicers has been facilitated by and is dependent on reliable access to the secondary mortgage market, mainly through federally supported securitization programs operated by the GSEs and Ginnie Mae. The increased market presence of nonbanks is evident in the share of originations delivered through these federally supported secondary market channels, with the nonbank share more than tripling between 2007 and 2016 to approximately 50% and 70% at the GSEs and Ginnie Mae, respectively.[274]

Figure 12: Depository v. Nondepository Share of All Mortgage Originations (percent)

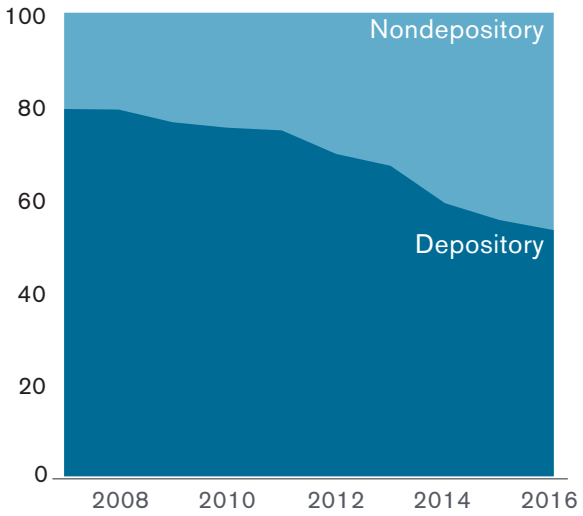
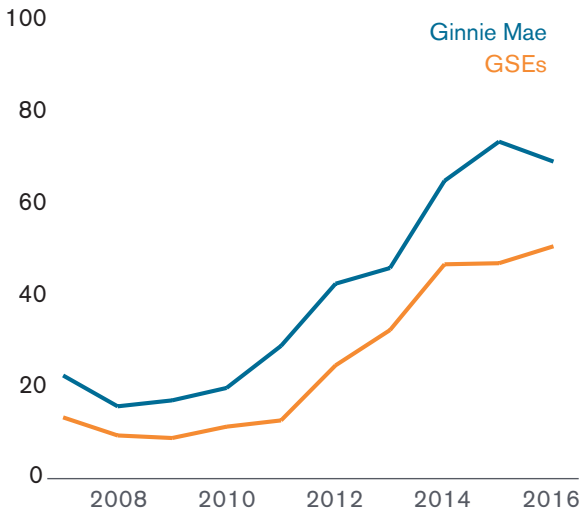


Figure 13: Nondepository Share of Mortgage Volume (percent)



Source: Home Mortgage Disclosure Act and Office of Financial Research analysis.

Many of these nonbank lenders have also been early adopters of financial technology innovations that speed up and simplify loan application and approval at the front end of the mortgage origination process.[275] Metrics associated with the loan origination process highlight the degree to which speed and cost-saving enhancements are possible, with average closing timelines stretching well beyond a month and requiring hours of costly, labor-intensive processes even as digitized, automated technology exists to mitigate these challenges. Research examining the impact of financial technology on mortgage origination is limited given the nascent state of adoption; however, early evidence suggests positive impacts from the use of automated, digital processes, with a recent study

274. HMDA and Office of Financial Research analysis.

275. Marshall Lux and Robert Greene, *What's Behind the Non-Bank Mortgage Boom?*, Harvard Kennedy School M-RCBG Associate Working Paper Series No. 42 (June 2015), available at: *https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/working.papers/42_Nonbank_Boom_Lux_Greene.pdf*.

finding that a digital front-end loan application shortened closing timelines by ten days or 20% of processing time without increasing default risk.[276]

While the growth of nondepository mortgage lenders and servicers has been supported by their early adoption of financial technology relative to their depository peers and access to the secondary mortgage market, nondepositories have also benefitted from the outright departure of many large depositories from certain segments of the mortgage market. This departure is concentrated in one of the key post-crisis channels to mortgage credit — the government-insured mortgage. Depositories have exited this market due to multiple factors that have unnecessarily raised the cost of engaging in this line of business, including substantial liability associated with the False Claims Act (FCA) and costly default servicing.[277]

Policymakers have an important role to play in the evolution of the mortgage lending and servicing marketplace by addressing regulatory challenges that discourage broad market participation and inhibit the adoption of beneficial technological developments. In its review of the impact of financial technology, innovation, and nonbanks on the mortgage market, Treasury has made the following findings:

- The adoption of financial technology and digital mortgage capabilities has the potential to improve the customer experience, shorten origination timelines, and deliver a more reliable, lower cost mortgage product;
- Current limitations on the acceptance of electronic mortgage promissory notes by key market participants limits the wider use and adoption of this technology, along with its attendant benefits for consumers and the marketplace;
- The mortgage production process is unnecessarily time intensive, with certain components prone to delays, which potentially could be relieved through policy changes conducive to further adoption of time- and cost-saving technology;
- State-level policy and regulatory differences across key components of the mortgage lifecycle create compliance uncertainty for lenders and servicers, increase costs, and inhibit the wider adoption of experience- and process-enhancing innovations;
- The use of the FCA to impose civil liability for violations of mortgage origination and servicing requirements has likely contributed to the exit of traditional commercial lenders from federal mortgage programs, raising the cost and limiting borrower access to mortgage credit for federally insured or guaranteed loans;
- Differences across loss mitigation programs and processes for federally supported mortgages, including those guaranteed or insured by the GSEs, Federal Housing Administration (FHA), U.S. Department of Veterans Affairs (VA), and U.S. Department of Agriculture (USDA), have the potential to negatively impact borrowers during periods

276. See Fuster et al., at 2.

277. See Neil Bhutta, Steven Laufer, and Daniel R. Ringo, Board of Governors of the Federal Reserve System, *The Decline in Lending to Lower-Income Borrowers by the Biggest Banks*, FEDS Notes (Sept. 28, 2017), available at: *https://www.federalreserve.gov/econres/notes/feds-notes/the-decline-in-lending-to-lower-income-borrowers-by-the-biggest-banks-20170928.htm*.

of financial hardship and could slow loss-mitigation responses during a subsequent period of sustained financial stress; and

- Federally supported mortgage programs exposed to nonbank counterparty credit risk could benefit from increased transparency into these counterparties' financial condition through greater standardization and reporting of key enterprise business and financial metrics.

Mortgage Lending and the Digital Mortgage

Originating a mortgage loan requires a multitude of interactions across counterparties, vendors, intermediaries, investors, settlement agents, service and data providers, and, most importantly, the borrower. Navigating this process can be frustrating for the housing finance industry as well as for borrowers at the point of origination and over the life of the loan.

Lenders typically manage mortgage loan production through a proprietary or third-party loan origination system, which acts as a system of record for the origination process, helps sequence workflow, and integrates with vendor services. In some instances, services are required by law — such as property appraisals for depository institutions.[278] In other cases, the requirements of federal insurance and guaranty programs, federally supported secondary market securitization programs, and the Federal Home Loan Banks (FHLBs) set de facto industry standards. These standards are particularly important for originators dependent on the liquidity and reliable access to the secondary market provided through these programs.

Across credit markets, technological advances — including the development of machine learning, database capabilities, and the implementation of more automated processes — are changing the manner, speed, and security of transactions. The use of information technology in the mortgage market has existed for decades; however, the industry has been slow to adopt innovations common in other consumer credit markets. While there is growing use of digital platforms for borrowers to shop and apply for a mortgage online, further digitization of the origination process beyond this first step, including through the use of electronic notes, closings, and recordings, remains limited. Where the use of electronic files has occurred, it has often been by incorporating scanned images of paper documents as opposed to developing fully digital files.[279] However, the application of financial technology in the mortgage market is accelerating, challenging existing norms as the industry transitions toward automated, digital practices and processes that appeal to customer demands in today's digital age.

Both depository and nondepository lenders are increasingly moving toward a digital front-end, either through proprietary platforms or commercially available products, as evidenced by increased borrower use in recent years. According to a 2017 survey conducted by J.D. Power, the number of borrowers utilizing the initial component of a digital front-end by submitting a mortgage

278. See e.g., 12 C.F.R. § 323.3.

279. See Margo H.K. Tank and R. David Whitaker, DLA Piper LLP, *Enabled by Lenders, Embraced by Borrowers, Enforced by the Courts: What You Need to Know About eNotes* (updated as of May 1, 2018), at 1, available at: *https://www.mersinc.org/media-room-docman/1419-enote-white-paper-final-09062017/file*.

application online increased from 28% in 2016 to 43% in 2017.[280] Fewer lenders at present have the capability to complete the digital front-end, instead using a digital application to trigger referral to a loan officer to continue the process in a more traditional paper-based, as opposed to fully digital, fashion.[281]

The capabilities to support a digital back-end mortgage process are even less developed. This stage comprises the more time- and labor-intensive portion of the production timeline and encompasses originator-driven activities from processing through loan closing, vendor services such as property appraisal and title insurance, and, ultimately, funding and sale into the secondary market. Further development of, and integration with, digital capabilities across the back-end of the process is integral to the ability for lenders to offer an end-to-end digital mortgage product. At present, this integration is challenged by disparate rules and non-uniform recognition of electronic and remote online notarizations, reticence by some county land-recording offices to accept digital property and security records, and still-developing industry capabilities to accommodate new technologies.

Challenges with Default Servicing, Loss Mitigation, and Foreclosure Practices

Post-crisis servicing rules administered by the Bureau have introduced a national standard for how delinquent loans are serviced; however, there remains significant differences in the loss mitigation products – such as loan modifications, short sales, and deeds-in-lieu of foreclosure – that are offered to delinquent borrowers. Generally, loss mitigation options made available to borrowers are established by the party most at risk for credit losses should the loan ultimately fail. In addition, loss mitigation options are influenced by other factors such as whether or not the loan is securitized and the requirements of the securitization program. Borrower and loan characteristics, as well as the level of market interest rates in relation to the borrower's current mortgage rate may also factor into the choice of an appropriate loss mitigation option. The fundamental differences between private investors, GSE guarantees, and government mortgage insurance programs result in a lack of standardization, which poses additional challenges for servicers when pursuing troubled loan workouts across servicing portfolios.[282] This inconsistency both directly impacts borrowers, who lack control over which entities purchase or service their loan, and ultimately dictates whether, and what type of, workout option is available in the event of financial hardship.

Servicers are additionally challenged by a lack of standardization in state-level foreclosure processes. Mortgage foreclosure processes are largely dictated by state law, which varies across the country. While some states have established statutory processes that permit a trustee to foreclose outside of court review, many other states require mediation and subject a foreclosure judgment to court review and approval, sometimes delaying the foreclosure process by years without improving borrower outcomes.

---

280. See J.D. Power, *Press Release – Despite a Rise in Use of Digital, Mortgage Customer Satisfaction Declines, J.D. Power Finds* (Nov. 9, 2017), available at: *http://www.jdpower.com/press-releases/jd-power-2017-us-primary-mortgage-origination-satisfaction-study*.

281. See Fuster et al., at 9.

282. See Laurie Goodman et al., *Government Loan Modifications: What Happens When Interest Rates Rise* (Jan. 2018), available at: *https://www.urban.org/sites/default/files/publication/95671/government-loan-modifications_2.pdf*.

For national mortgage servicers, managing to these unique requirements creates added costs when an aligned standard could deliver equally effective, or improved, outcomes for participants. In the face of these challenges, servicers may allocate resources to compliance as opposed to developing more effective mortgage-servicing platforms and deploying technology that would improve the borrower experience, particularly for those borrowers in default.

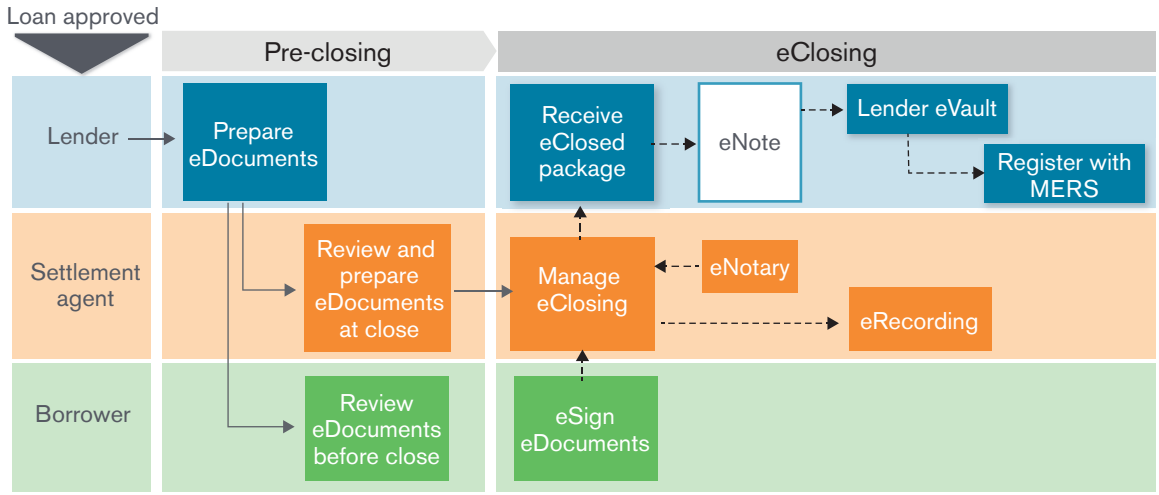
Issues and Recommendations

Electronic Mortgage Notes

The negotiable promissory note between lender and borrower is central to the mortgage origination process and establishes the borrower's obligation to repay the lender for funds lent to purchase or refinance a home. At present, the vast majority of promissory notes are paper-based, "wet signed" by lender and borrower, and subsequently physically stored and transmitted. A fully electronic mortgage note, often referred to as an eNote, is an electronic version of the negotiable promissory note that is digitally signed and electronically transmitted and stored. The eNote forms the main digital component of an electronic mortgage, or eMortgage, which comprises a full end-to-end mortgage transaction that can be completed entirely through digital means.

Digital mortgage notes have a clear statutory basis in the Electronic Signatures in Global and National Commerce Act of 2000 (ESIGN), which recognized the legal validity of signatures and records executed with an electronic stamp as opposed to a wet signature on paper,[283] and in the 1999 Uniform Electronic Transactions Act (UETA), by which the National Conference of Commissioners on Uniform State Laws proposed uniform rules for state adoption of laws

Figure 14: Illustrative eNote Process



Source: Fannie Mae and Treasury.

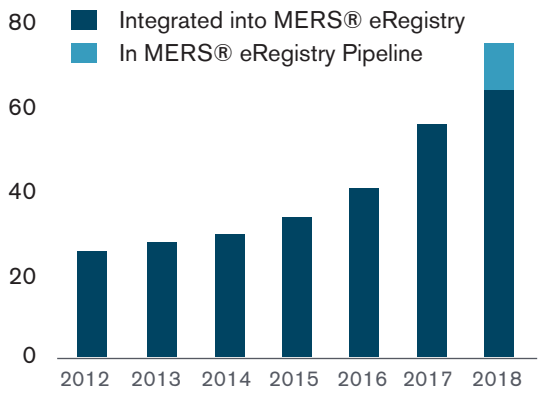
283. 15 U.S.C. §§ 7001-7031.

recognizing electronic records on an equal basis with paper ones.[284] Case law in the years since the passage of these eCommerce laws has upheld the legal enforceability of digital mortgage notes.[285]

eNotes require a digital promissory note to be electronically created, signed, secured, and registered, with maintenance in an electronic registry, or eRegistry, of the party in control of the note and the location of the authoritative copy of the registered note. Parties to an eNote, or their designated document custodian, store their versions of the eNote in a secure digital vault referred to as an eVault, with the location of the copy of record designated and maintained by the electronic registry itself. The MERS® eRegistry is utilized as the industry standard registry service for complying with the provisions of the eCommerce laws as a system of record for identifying the controller and location of the authoritative copy of the eNote and is recognized as such in the text of the Note itself.

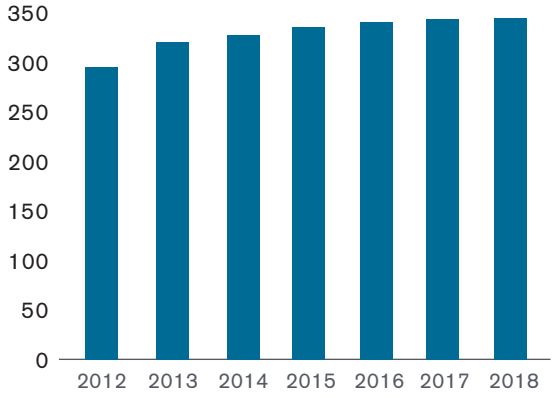
The framework, practices, and basis for eNotes is well established, even as adoption is limited. Secondary market investors Fannie Mae and Freddie Mac have had guidelines in place for approving a lender for and purchasing eNotes since the early 2000s. Primary market development of eNote capabilities was likely sidelined by the financial crisis and the subsequent wave of post-crisis regulations, which required capital resources and process updates. Today, there are 26 seller-servicers approved to deliver eNotes to the GSEs.[286] eNote deliveries represented less than 1% of 2017 GSE acquisition volumes.[287] However, as illustrated by **Figures 15** and **16**, both the number of companies integrated with the MERS® eRegistry and the number of eNotes registered on it has grown in recent years, consistent with the burgeoning interest in and development of this capability.

Figure 15: Number of Companies Active on the MERS® eRegistry



Source: MERSCORP Holdings, Inc.

Figure 16: Cumulative Number of eNotes Registered on the MERS® eRegistry (thousands)



Source: MERSCORP Holdings, Inc.

284. See National Conference of Commissioners on Uniform State Laws, *Uniform Electronic Transactions Act (1999)*, available at: *http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf*

285. See Tank and Whitaker, at 9.

286. Data provided by the Federal Housing Finance Agency (FHFA).

287. Id.

Electronic promissory notes offer advantages over their analog versions that accrue to both the mortgage industry and borrowers. The ability to digitally execute this component of the origination process aligns with broader industry migration to digital capabilities and offers convenience, more efficient quality control, and, when integrated with a broader eMortgage solution, faster origination timelines. More specifically, eNotes are more readily transferred between holders as they are bought and sold in the secondary market, they cost less to store and transmit than paper notes, and they offer greater protection against unauthorized tampering, alteration, or loss.

Primary market development of the capability to originate eNotes represents one barrier to their wider adoption. An additional reason for their limited use is their lack of acceptance by other key secondary market participants. For federally insured mortgages from the FHA and VA, lenders generally prefer to securitize and issue Ginnie Mae mortgage securities. However, Ginnie Mae stated in an All Participant Memorandum in February 2014 that it was concerned with maintaining the liquidity and negotiability of its pools and would not allow electronic signatures or electronic documents on promissory notes, security instruments, or loan modification agreements.[288] More recently, Ginnie Mae has stated its commitment to developing its digital capabilities, including the eventual acceptance of digital promissory notes into its pools.[289]

Both FHA and VA have accepted digital signatures on notes since 2014 and 2013, respectively.[290] However, FHA in particular is challenged by an aging technology infrastructure that limits its ability to process and store digital loan files, mitigating the use of eNotes or broader digital mortgage files, and inhibiting lenders from offering this capability for government-supported loans.[291] As loans insured or guaranteed by FHA and VA comprise nearly a quarter of new originations, any limited functionality with regard to digital mortgage files acts as a barrier on wider industry adoption.

The FHLBs' lack of acceptance of eNotes represents an additional barrier to their further use. The FHLBs' primary business is providing secured advances to member institutions that support mortgage lending activity. The FHLBs currently do not accept eNotes as eligible, pledged collateral from their members for securing an advance.[292] While the FHLBs have expressed interest moving toward the acceptance of eNotes, they have identified two primary issues to address: (1) the current limited depth of a secondary market for eNotes; and (2) the appropriate representation for the FHLBs in the MERS® eRegistry where they have an interest in, but are not the owner of, eNotes as pledged collateral. In response to this concern, MERSCORP Holdings, Inc., is pursuing

---

288. Ginnie Mae, *All Participant Memorandum 14-01: Electronic Notes and Mortgages* (Feb. 27, 2014), available at: *https://www.ginniemae.gov/issuers/program_guidelines/Pages/mbsguideapmslibdisppage.aspx?ParamID=24*.

289. Ginnie Mae, *Ginnie Mae 2020* (June 2018), available at: *https://www.ginniemae.gov/newsroom/publications/Documents/ginniemae_2020.pdf*.

290. U.S. Department of Housing and Urban Development, *Electronic Signatures*, Mortgagee Letter 2014-03 (Jan. 30, 2014), available at: *https://www.hud.gov/sites/documents/14-03ML.PDF;* Veterans Benefits Administration, *Use of Electronic Signatures in Conjunction with Department of Veterans Affairs (VA) Guaranteed Home Loans*, Circular 26-13-13 (Aug. 22, 2013), available at: *https://www.benefits.va.gov/homeloans/documents/circulars/26_13_13.pdf*.

291. See FHA *Annual Management Report: Fiscal Year 2017* (Nov. 27, 2017), available at: *https://www.hud.gov/sites/documents/FHAFY2017ANNUALMGMNTRPT.PDF*.

292. See Federal Home Loan Bank of Des Moines, *Collateral Quarterly* (Aug. 24, 2017), available at: *https://members.fhlbdm.com/media/cms/pages_fhlbdm_com_rs_171_ZQM_109_ima_09B7E4A798CA0.pdf*.

the addition of a new Secured Party field to its eRegistry, which will enable certain parties, such as FHLBs and warehouse lenders, to be more appropriately represented in alignment with their position in the mortgage process today.[293]

Recommendations

Treasury recommends that Ginnie Mae pursue acceptance of eNotes and supports the measures outlined in its *Ginnie Mae 2020* roadmap to more broadly develop its digital capabilities.

FHA is limited by its congressionally-appropriated budget but is in need of technology overhauls beyond the narrower discussion of digital mortgage capabilities. Treasury recommends that Congress appropriate for FHA the funding it has requested for technology upgrades in the President's Fiscal Year 2019 Budget — a portion of which FHA would use to improve the digitization of loan files.[294] In addition, FHA, VA, and USDA should explore the development of shared technology platforms, including for certain origination and servicing activities.

Finally, Treasury recommends the FHLBs explore ways to address their concerns regarding eNotes with the goal of accepting eNotes on collateral pledged to secure advances.

Appraisals

Property appraisal practices, including a perceived lack of appraiser independence from loan originators and insufficiently stringent qualification requirements, were criticized in connection with the housing bubble and subsequent collapse in home prices. In response, lawmakers and regulators enacted changes to appraisal requirements that have fundamentally affected the appraisal industry. In recent years, lenders and homebuyers have pointed to the appraisal component of the origination process as a frequent source of delays and a driver of extended closing timelines.[295]

Concurrently, advances in financial technology, particularly with regard to automated valuation models (AVMs), have pushed appraisals in a new and innovative direction. The application of this technology has already begun to disintermediate the traditional appraisal process and, notably, has been adopted by both GSEs. The digitization of this component of the origination process, facilitated through electronic property records, development of large databases capable of holding millions of individual property records, and improvement of advanced valuation algorithms, holds promise to lower cost and expedite closing timelines.

Property appraisal standards for federally related real-estate transactions are governed by Title XI of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA).[296] In order to protect deposit insurance funds and to promote prudent lending, FIRREA assigned to the Appraisal Subcommittee of the Federal Financial Institutions Examination Council the

---

293. This new field, as described by MERSCORP Holdings, Inc., would represent the entity that has been assigned or granted an interest in the eNote by the Controller.

294. See U.S. Department of Housing and Urban Development, *FY 2019 Congressional Justification*, at 26-1 to 26-7, available at: *https://www.hud.gov/program_offices/cfo/reports/fy19_CJ*.

295. See National Association of Realtors, *Realtors Confidence Index Survey* (Apr. 2018), at 7, available at: *https://www.nar.realtor/research-and-statistics/research-reports/realtors-confidence-index*.

296. Public Law No. 101-73, Title XI [codified at 12 U.S.C. §§ 3331-3355].

responsibilities to monitor state-level appraiser standards and credentialing, maintain a national registry of certified and licensed appraisers, and oversee the practices, procedures, and activities of the Appraisal Foundation, among other duties.[297]

FIRREA delegated to the Appraisal Foundation — a nonprofit industry organization — authority to set property valuation standards and minimum appraiser qualification requirements.[298] The Appraisal Foundation fulfills this mandate through two independent boards – the Appraisal Standards Board (ASB), which sets appraisal practices, and the Appraiser Qualifications Board (AQB), which establishes minimum state-level credentialing requirements.[299] These standards are binding for transactions by lenders subject to FIRREA, but are also used broadly throughout the housing finance system, including by the FHA and the GSEs.

The ASB maintains the Uniform Standards of Professional Appraisal Practice (USPAP), which sets ethical and professional standards for appraisers operating in the United States.[300] The AQB dictates minimum qualification criteria, with credentials tiered into classifications, with most real-estate transactions requiring appraisal by either a state-licensed residential real property appraiser or a state-certified real property appraiser, with each classification becoming progressively more selective.[301] Until May 2018, to become a certified residential appraiser, an individual would need to have completed a minimum four-year bachelor's degree, while licensed appraisers were subject to lesser college-level education requirements.[302] The AQB has recently implemented changes to ease the education requirements by removing the college education requirement for licensed appraisers and reducing the bachelor's level requirement for certified appraisers.[303]

The prudential banking regulators have, in the years since FIRREA's enactment, established numerous exemptions from the statutory appraisal requirement.[304] Through these Interagency Appraisal and Evaluation Guidelines, financial institutions subject to FIRREA may undertake a property evaluation in lieu of an appraisal for prescribed transactions, including single-family residential transactions where the market value is less than $250,000, commercial real estate transactions less than $500,000, certain refinancings, and where the transaction is guaranteed by or eligible for guarantee by a U.S. government agency or government-sponsored agency.[305]

---

297. 12 U.S.C. § 3332.

298. 12 U.S.C. §§ 3339, 3345.

299. See The Appraisal Foundation, available at: *https://www.appraisalfoundation.org/imis/TAF/About_Us/TAF/About_Us.aspx?hkey=52dedd0a-de2f-4e2d-9efb-51ec94884a91*.

300. See Appraisal Standards Board, *2018-2019 Uniform Standards of Professional Appraisal Practice (USPAP)*, available at: *http://www.uspap.org/files/assets/basic-html/page-1.html#*.

301. See The Appraisal Foundation, *The Real Property Appraiser Qualification Criteria* (May 1, 2018), available at: *https://appraisalfoundation.sharefile.com/share/view/scbea7640298440aa*.

302. See Appraiser Qualifications Board, *Summary of Changes to the Real Property Appraiser Qualification Criteria* (May 1, 2018), available at: *https://appraisalfoundation.sharefile.com/share/view/s40e607fb0d64915a*.

303. Id.

304. See Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, and National Credit Union Administration, *Interagency Appraisal and Evaluation Guidelines* (Dec. 2, 2010), available at: *https://www.fdic.gov/news/news/financial/2010/fil10082a.pdf*; see also 12 C.F.R. § 323.3.

305. Id.

The GSEs and federal housing programs, administered, for example, by FHA, act as de facto standard setters for mortgage appraisal requirements performed by both depositories, through the FIRREA exemption, and the large segment of nondepository lenders not subject to FIRREA. Lenders originating government mortgage loans, such as those insured by FHA or guaranteed by the VA or USDA, are required to comply with the appraisal policies established by these programs.[306] Fannie Mae's and Freddie Mac's seller-servicer guides similarly establish minimum eligibility standards for appraisals to qualify for purchase by the respective GSE. Both FHA and the GSEs require a USPAP-compliant appraisal for nearly all purchase and refinance loans.[307]

In 2017, Fannie Mae and Freddie Mac began offering originators appraisal waivers on a limited population of purchase and refinance loans.[308] The GSEs offer these waivers by leveraging their proprietary appraisal models and databases aggregating public records, multiple listing services, and millions of appraisal reports delivered electronically to the GSEs since 2012. For loans that qualify for the waiver, the originator may forego the appraisal component of the loan production process, potentially shortening timelines by as much as 10 days, and reducing origination costs by up to $700.[309]

Independent appraisers highlight post-crisis changes as exacerbating a mismatch between lender demand for appraisal servicers and the number of independent appraisers qualified and willing to meet this demand. Post-crisis appraiser independence standards enacted under Dodd-Frank have resulted in lenders channeling appraisal requests through appraisal management companies (AMCs) to subcontract with a state-licensed or state-certified appraiser.[310] Partly as a result of more widespread use of AMCs as a market intermediary, independent appraisers report being paid relatively less than they earned prior to the introduction of the appraisal independence standard that gave rise to increased use of AMCs. Appraisers in some areas may be reticent to accept appraisal requests due to the compensation passed through to them. Delays in completing an origination or upcharges for rush appraisals to meet closing timelines may result and are ultimately borne by the borrower through higher origination costs.

Against this backdrop, the development of new appraisal technology offers the potential, when used responsibly, to relieve some of the pressures in the appraisal market and reduce the time and cost necessary to complete a property appraisal. This technology ranges from approaches that supplement traditional appraisals with remote evaluation technology to the deployment of AVMs to remotely estimate property value without recourse to in-person appraisers. AVMs

---

306. See U.S. Department of Housing and Urban Development, *FHA Single Family Housing Policy Handbook 4000.1* (Dec. 30, 2016), at Section II.D, available at: *https://www.hud.gov/sites/documents/40001HSGH.PDF* ("FHA Single Family Handbook").

307. See Fannie Mae, *Selling Guide* (June 5, 2018), at Part B4-1, available at: *https://www.fanniemae.com/content/guide/selling/b/index.html*; see Freddie Mac, *Single-Family Seller/Servicer Guide* (June 13, 2018), at Ch. 5601, available at: *http://www.freddiemac.com/singlefamily/pdf/guide.pdf*.

308. See Fannie Mae*, Property Inspection Waiver*, available at: *https://www.fanniemae.com/singlefamily/property-inspection-waiver*; Freddie Mac, *Automated Collateral Evaluation Now Available for Purchase Transactions*, available at: *http://www.freddiemac.com/singlefamily/news/2017/0818_ace_purchases.html*.

309. See Freddie Mac, *Automated Collateral Evaluation (ACE)*, available at: *http://www.freddiemac.com/singlefamily/loanadvisorsuite/pdf/ACEMatrixDoc.pdf*.

310. 15 U.S.C. § 1639e.

have existed for several decades but their use and accuracy has improved in recent years due to advances in machine learning, database technologies, and the proliferation of large datasets composed of proprietary and public records with detailed property-specific information. At present, AVMs are not permitted in place of traditional in-person appraisals for most loans sold to the GSEs, endorsed by FHA or insured by other government loan programs, or for real-estate transactions subject to FIRREA.

Critics of traditional appraisals argue that they represent an outdated and costly approach relative to new digital tools. Critics of AVMs argue that they are dependent on detailed data provided by an appraiser in order to maintain AVM accuracy, and that the disintermediation of traditional appraisals will degrade AVMs as a result. Another form of property appraisal exists between these two approaches to combine aspects of traditional appraisals with the automation and database capabilities of AVMs. So-called hybrid or desktop appraisals leverage property history data, comparable sales data, photographs or video of the interior and exterior of a property, and a licensed or certified appraiser. As the name would imply, desktop appraisals are able to be executed from a single remote location, and offer the potential to save appraisers considerable time that would otherwise be spent in transit to and from properties.

Recommendations

Treasury recommends that Congress revisit Title XI FIRREA appraisal requirements to update them for developments that have occurred in the market during the past thirty years. Recent data has illustrated that approximately 90% of residential mortgage originations are eligible for appraisal exceptions established since the enactment of FIRREA by the designated federal regulatory agencies.[311] An updated appraisal statute should account for the development of automated and hybrid appraisal practices and sanction their use where the characteristics of the transaction and market conditions indicate it is prudent to do so.

Treasury supports the GSEs' efforts to implement standardized appraisal reporting, the GSEs' and FHA's adoption of proprietary electronic portals to submit appraisal forms, and the GSEs' limited adoption of appraisal waivers. While Treasury acknowledges that automated valuation engines and appraisal waivers should apply to a defined and limited subset of loans, and that they may compete with traditional appraisers, these innovations offer borrowers upside through lower cost originations and faster closings, without sacrificing accuracy. However, further application of digital, automated property valuations must be carefully monitored and integrated with rigorous market standards where they are used in lieu of traditional appraisals.

Treasury recommends FHA and other government loan programs develop enhanced automated appraisal capabilities to improve origination quality and mitigate the credit risk of overvaluation. These programs may also wish to consider providing targeted appraisal waivers where a high degree of property standardization and information about credit risk exists to support automated valuation, and where the overall risks of the mortgage transaction make such a waiver appropriate. Treasury supports legislative action where statutory changes are required to authorize granting

311. See Federal Financial Institutions Examination Council, *Joint Report to Congress: Economic Growth and Regulatory Paperwork Reduction Act* (Mar. 2017), available at: *https://www.occ.gov/news-issuances/news-releases/2017/nr-ia-2017-33a.pdf*.

limited appraisal waivers for government programs. Treasury further recommends that government loan programs explore opportunities to leverage industry-leading technology capabilities to reduce costs to taxpayers and accelerate adoption of new technology in the government-insured sector.

Finally, Treasury supports the AQB's recently updated appraisal certification guidelines that ease the education requirements to obtain that credential, with the understanding that providing off-ramps for the education requirement in favor of on-the-job training or other education credits can attract qualified appraisers to this industry and relieve appraiser supply challenges without jeopardizing valuation credibility.

Electronic Closing and Recording

Mortgage closing, or settlement, represents the last step for a borrower in financing a home, and comprises the execution of the financial and title documents that form the basis for the mortgage loan and transfer of claim to the property. A key component of the closing process is the notarization of real estate transfer documents, such as the deed, which are subsequently filed, or publicly recorded, with local county land records. Traditionally, the loan closing is completed in one sitting, with the borrower and parties to the transaction physically present in the same location.

Notarization methods have expanded along with the rest of electronic commerce in recent decades and can now be accomplished either in-person through a digital document and notary seal or remotely through online interaction via webcam and using knowledge-based identification to confirm the borrower's identity. According to the Bureau's 2015 eClosing pilot, the ability to electronically complete the mortgage process through digital notarization represents one of the key remaining impediments to the digital process and offers additional borrower convenience and satisfaction if executed seamlessly versus a paper-based closing.[312]

While the UETA and ESIGN eCommerce laws establish the validity of electronic signatures on consumer credit transactions, additional legal clarity is needed to ensure compliance with state notary laws for use of electronic notarizations, specifically the sanctioning of digital notarizations in lieu of a physical signature and notarization. To date, 39 states have enacted laws establishing the legality of such eNotarization.[313] In 2010, in part to account for the development of eNotarization capabilities, the National Conference of Commissioners on Uniform State Laws (also known as the Uniform Law Commission, or ULC) promulgated a revised model statutory framework for notarial acts, updating its original 1982 model act and aimed at facilitating interstate recognition of various types of notarizations.[314] To date, 11 states have enacted the revised Uniform Law Commission framework.[315]

---

312. See Bureau of Consumer Financial Protection, *Leveraging Technology to Empower Mortgage Consumers at Closing* (Aug. 2015), available at: *https://files.consumerfinance.gov/f/201508_cfpb_leveraging-technology-to-empower-mortgage-consumers-at-closing.pdf*.

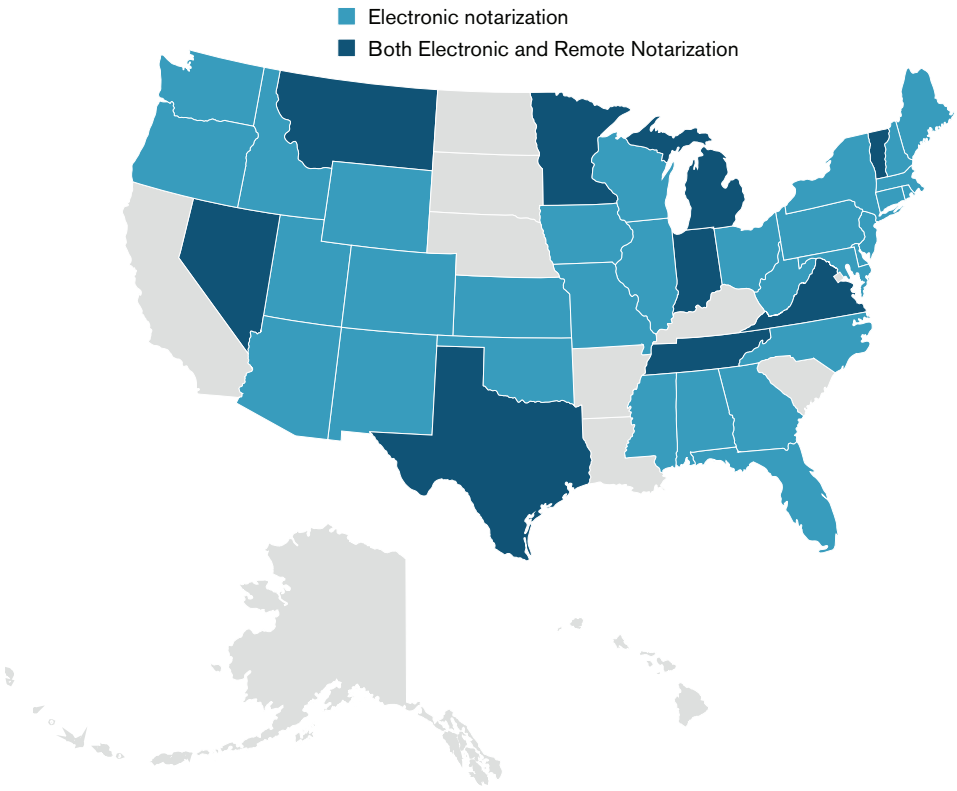
313. Based on information provided by the American Land Title Association to Treasury.

314. See Uniform Law Commission, *Revised Uniform Law on Notarial Acts* (2010), available at: *http://www.uniformlaws.org/Act.aspx?title=Law%20on%20Notarial%20Acts,%20Revised*.

315. Id.

These electronic notarization statutes, enabling digital notary signature for in-person notarizations, provide insufficient legal certainty for the use of remote notarization conducted electronically via webcam, with the latter permitting both signatory and notary to be in different locations. Virginia became the first state to officially sanction remote online notarization when it passed legislation to that end in 2012. Seven other states have followed suit, while an additional four states have remote online notarization bills pending, with the potential for passage in 2018.[316] In 2017, the American Land Title Association and the Mortgage Bankers Association (MBA), in an effort to address legal uncertainty and to facilitate further development of eMortgage capabilities, published model legislation providing a framework for states to use in adopting remote online notarization for real-estate transactions.[317]

Figure 17: Electronic and Remote Notarization by State



Source: American Land Title Association and Treasury staff analysis.

316. See Mortgage Bankers Association, *Remote Online Notarization*, available at: *https://www.mba.org/audience/state-legislative-and-regulatory-resource-center/remote-online-notarization* (last accessed June 14, 2018).

317. See American Land Title Association, *ALTA, MBA Develop Model Legislation for Remote Online Notarization* (Dec. 19, 2017), available at: *https://www.alta.org/news/news.cfm?20171219-ALTA-MBA-Develop-Model-Legislation-for-Remote-Online-Notarization*.

Despite state-level progress toward wider recognition of electronic notarization, the absence of a broad statutory acceptance across the country and uneven standards for remote and electronic notarization implementation has created confusion for market participants, slowing adoption of digital advances in mortgage technology by limiting the ability for lenders to complete a digital mortgage with an eClosing. Non-uniform state rules create a cost barrier for electronic notarization system vendors developing their platforms and creates uncertainty for investors considering purchasing digital mortgages. In 2006, the National Association of the Secretaries of State adopted standards for state use in implementing in-person, electronic notarizations. Amendments to these standards, accounting for the advance of remote notarizations, were recently adopted in February 2018 to support secure and technology-neutral implementation of remote notarization capabilities.[318]

County-level acceptance of digital security instruments is a key determinant of whether a lender will pursue an electronic closing, as lack of acceptance of these documents renders such critical eMortgage components, such as electronic notarization, moot. In 2004, the Uniform Law Commission promulgated the Uniform Real Property Electronic Recording Act (URPERA), representing a model statutory framework to provide county clerks and recorders the authority to accept electronic recording of real property instruments. Today, 33 states and U.S. territories have enacted URPERA; however, implementation remains a county-level exercise.[319] As of May 31, 2018, just over half of the 3,600 recording jurisdictions—primarily, but not exclusively counties—in the United States offer electronic recording.[320] Greater digitization of property records at the county level may, in the future, facilitate further advances in mortgage technology, including the potential application of distributed ledger technology to more expeditiously perform property record checks and expedite title review services.

Recommendations

Treasury recommends that states yet to authorize electronic and remote online notarization pursue legislation to explicitly permit the application of this technology and the interstate recognition of remotely notarized documents. Treasury recommends that states align laws and regulations to further standardize notarization practices.

Treasury further recommends that Congress consider legislation to provide a minimum uniform national standard for electronic and remote online notarizations. Such legislation would facilitate, but not require, this component of a fully digital mortgage process and would provide a greater degree of legal certainty across the country. Federal legislation is not mutually exclusive with continued efforts at the state level to enact a framework governing the use of electronic methods for financial documents requiring notarization.

---

318. See National Association of Secretaries of State, *NASS Support for the Revised National Electronic Notarization Standards* (amended and readopted on Feb. 19, 2018), available at: *https://www.nass.org/node/1327*.

319. See Uniform Law Commission, *Real Property Electronic Recording Act*, available at: *http://www.uniformlaws.org/Act.aspx?title=Real%20Property%20Electronic%20Recording%20Act*.

320. See Property Records Industry Association, available at: *https://www.pria.us/i4a/pages/index.cfm?pageid=1* (last accessed on June 14, 2018).

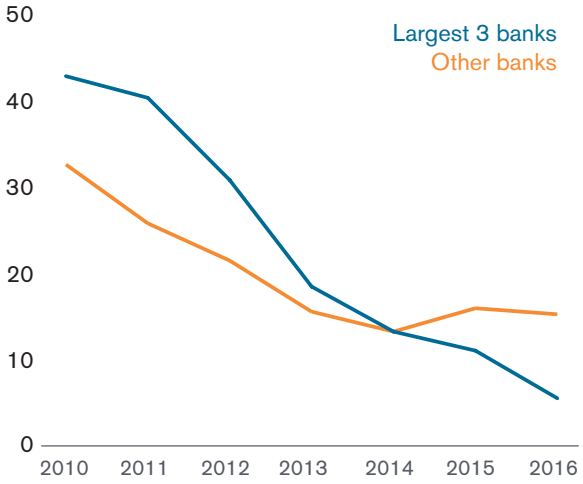
Treasury recommends that recording jurisdictions yet to recognize and accept electronic records implement the necessary technology updates to process and record these documents and to pursue digitization of existing property records.

False Claims Act

Civil actions brought under the authority of the False Claims Act (FCA) — a Civil War-era statute — have been closely associated with the mortgage industry since the financial crisis. Beginning in 2011, the U.S. Department of Justice (DOJ), often based on a referral from the Inspector General for the U.S. Department of Housing and Urban Development (HUD), has pursued numerous claims under the FCA against lenders of government mortgages where it was determined that the lenders knowingly submitted for government insurance mortgages that did not meet federal eligibility standards.

DOJ has recovered approximately $7 billion related to FCA housing fraud settlements and judgments to date.[321] The cost of FCA liability for lenders and servicers, and the ongoing fear of future action by the government is often cited as a factor in the shift away from depositories and toward nondepository mortgage banks in the government mortgage loan market.[322] The departure of depositories from federally insured mortgages has likely had negative impacts on borrower access to credit by reducing the available lending universe and encouraging remaining lenders to add credit and risk overlays to their underwriting to mitigate lower credit quality, but nonetheless creditworthy, borrowers.

Figure 18: FHA Share of Originations (percent)



Source: Federal Reserve (see Bhutta et al.) using HMDA data.

An entity that violates the FCA by knowingly submitting false claims to the government is subject to substantial civil remedies: penalties between $11,181 and $22,363 per false claim as well as triple the amount of damages to the government — known as treble damages.[323] Furthermore, it has been standard practice for DOJ to determine the percentage incidence of errors on a sample size of loans that have gone to claim and then extrapolate the incidence of violations to a broader population of loans that went to claim to capture what DOJ alleges to be the full extent of the false claims submitted by lenders and servicers. Because the FCA only allows a recovery when a loan defaults and results in a claim for mortgage insurance, the samples selected in FCA actions are only drawn from the

321. See U.S. Department of Justice, *Fact Sheet: Significant False Claims Act Settlements & Judgments, Fiscal Years 2009–2016*, available at: *https://www.justice.gov/opa/press-release/file/918366/download*.

322. See Bhutta, Laufer, and Ringo.

323. 31 U.S.C. § 3729(a)(1).

universe of loans that went to claim. Thus, the samples are not intended, and cannot be interpreted, to be representative of a lender's overall portfolio.

Before liability or damages may be imposed under the FCA, the FCA requires that any false claim be both knowing and material.[324] Consistent with this latter requirement, DOJ and HUD have a practice of reaching mutual agreement on resolving claims, even though the process by which agreement is reached has been characterized as lacking clarity. DOJ's FCA settlements have often been accompanied by admitted statements of facts by the settling lenders, and these statements have confirmed the lenders' knowledge of the materiality of the defects that were the subject of the settlements.[325] Nevertheless, HUD and DOJ have been criticized for not sufficiently differentiating knowing and material errors from those that would not have affected approval of the loan for a federal program or servicer actions during the foreclosure process.[326] Distinguishing knowing and material errors from clerical defects is particularly important to lenders and servicers. Even if lenders and servicers strive to ensure the information they collect and submit to FHA is complete and accurate, minor errors are to be expected. Industry concerns about being held liable under the FCA for these types of defects may affect the decision to participate, and at what price, in government loan programs.

HUD has taken steps in recent years to provide additional clarity around the severity across violations and to provide lenders greater certainty that loans they originate and service are insurable by the FHA. Administrative changes to loan-level certifications and implementation of a loan quality review taxonomy were executed in an attempt to encourage lenders to re-enter the FHA market by clarifying a materiality threshold for errors.

FHA lenders are required to certify annually that they meet established HUD-FHA approval standards. Additionally, lenders must certify at the loan-level that loans meet FHA eligibility requirements. In 2016, HUD updated its loan-level certification, which attempted to apply a materiality threshold to instances where violations would trigger the rescission of FHA insurance by defining liability as errors that would have altered the decision to approve a loan.[327] More significantly, in 2017, FHA announced the implementation of its Loan Review System, incorporating the Loan Quality Assessment Methodology (Defect Taxonomy).[328] The Defect Taxonomy classifies nine defect areas by category, identifies the source and cause of the defect, and classifies them into four severity tiers based on the nature of the error, with errors moving from most severe in tier

---

324. Id.; *Universal Health Services v. United States ex rel. Escobar*, 136 S. Ct. 1989 (2016).

325. See *The False Claims Act & Federal Housing Administration Lending* (March 15, 2016), available at *https://www.justice.gov/archives/opa/blog/false-claims-act-federal-housing-administration-lending*.

326. See Paul Compton, Jr., U.S. Department of Housing and Urban Development, *New Era of Cooperation and Coordination* (Apr. 30, 2018), available at: *https://www.hud.gov/press/speeches_remarks_statements/Speech_043018*.

327. See U.S. Department of Housing and Urban Development, *Revised HUD 92900-A HUD/VA Addendum to Uniform Residential Loan Application,* Mortgagee Letter 2016-06 (Mar. 15, 2016), available at: *https://www.hud.gov/sites/documents/16-06ML.PDF*.

328. See U.S. Department of Housing and Urban Development, *Federal Housing Administration (FHA) Loan Review System – Implementation and Process Changes*, Mortgagee Letter 2017-03 (Jan. 11, 2017), available at: *https://www.hud.gov/sites/documents/17-03ML.PDF*.

one to the least severe in tier four.[329] With this taxonomy, FHA intended to clarify the severity of loan-level violations — distinguishing material defects from errors that would not impact the insurability of the loan.

While industry participants have been supportive of providing additional clarity around what constitutes a manufacturing defect and the nature of the defect, stakeholders have called for HUD and FHA to take the further administrative step of providing a prescribed remedy for each violation in the taxonomy and a safe harbor for violations at the lower tiers of the taxonomy and for those at the higher tiers that have been cured. Furthermore, many market participants feel that action by FHA alone is insufficient to relieve lender concerns about liability tail risk. For example, the Defect Taxonomy has not altered the eligibility rules for HUD loans, which means it does not govern when DOJ can or should bring appropriate FCA claims. To market participants seeking to mitigate risk of FCA liability, the fact that FHA may differentiate violations based on materiality in its own administrative proceedings offers no guarantee that DOJ, or a whistleblower litigating a qui tam action in place of the government, will adopt the same posture. Since the Supreme Court's decision in *Universal Health Services v. United States ex rel. Escobar*, the views of the agency making payment decisions significantly affect determinations of materiality (or lack thereof).[330] Even following the Escobar ruling, the industry would benefit from additional clarity on the common standards applied by HUD and DOJ.

Material errors in manufacturing and servicing government loans should continue to be subject to enforcement by FHA and DOJ and bad actors who knowingly defraud the government should face significant fines and penalties. But when industry is reluctant to originate or service government loans in light of the FCA enforcement risk, this serves the counterproductive end of increasing the cost of credit and potentially limiting borrower access to federal loan programs.

Recommendations

Enforcement of the FCA is critical to ensuring the integrity of any federal program and protecting it against knowing violations. At the same time, FCA enforcement actions can impose significant costs on a defendant both in terms of financial and reputational damages. Accordingly, it is important that an appropriate balance be struck between what program requirements an agency considers to be material – and therefore subject to potential FCA enforcement when knowing violations of these requirements occur – and what requirements are not material, and are appropriately addressed through actions outside of the FCA.

To address the perception associated with the use of the FCA on mortgage loans insured by the federal government, Treasury recommends that HUD establish more transparent standards in determining which program requirements and violations it considers to be material to assist DOJ in determining which knowing defects to pursue. In doing so, Treasury recommends that FHA clarify the remedies and liability lenders and servicers face, which could include, where appropriate, remedies such as indemnification and/or premium adjustments. Remedies should be correlated to

329. See FHA's Single Family Housing Loan Quality Assessment Methodology, available at: *https://www.hud.gov/sites/documents/SFH_LQA_METHODOLOGY.PDF*.

330. See Escobar, 136 S. Ct. at 1989.

the Defect Taxonomy. FHA should continue to review and refine its lender and loan certifications and its loan review system, including the Defect Taxonomy. Lenders that make errors deemed immaterial to loan approval should receive a safe harbor from a denial of claim and forfeiture of premiums. Lenders should receive a similar safe harbor for material violations that are cured based on remedies prescribed by FHA absent patterns which indicate a systemic issue. In determining the appropriate remedies for violations of its program requirements, HUD should consider the systemic nature of the problem, involvement or knowledge of the lender's senior management, overall quality of the originations of a specific lender, and whether or to what extent the loan defect may have impacted the incidence or severity of the loan default.

Treasury recommends DOJ ensure that materiality for purposes of the FCA is linked to the standards in place at the agency administering the program to which the claim has been filed, and that DOJ and HUD work together to clarify the process by which mutual agreement is reached on the resolution of claims. Where a relator pursues *qui tam* action against a lender for a nonmaterial error or omission, DOJ, in consultation with HUD and FHA, should consider exercising its statutory authority to seek dismissal.[331]

Distinguishing materiality, providing clear remedies to cure discovered defects, and linking the Defect Taxonomy to the FCA could provide a measure of certainty that could attract lenders back into this market and reduce costly overlays without constraining the government's ability to punish bad actors and prosecute knowingly fraudulent activity. However, if the recommended administrative actions are unsuccessful at achieving the desired result of increasing lender and servicer participation in federal mortgage programs, Congress should consider appropriate remedial legislation.

Aligned Federal Mortgage Loss Mitigation Standards

The Bureau has implemented multiple servicing rules and rule revisions during the past five years, requiring numerous changes to servicer procedures, particularly concerning procedures for how to engage delinquent borrowers when evaluating them for loan modifications or other loss mitigation options. The federal government has not promulgated rules to prescribe a national loss mitigation standard. Crisis-era loss mitigation programs offered a degree of standardization and transparency for servicers, borrowers, and mortgage investors around loss mitigation options. In the absence of such a de facto federal loss mitigation standard, some market participants have cited concerns with the variance in options across different federal mortgage programs.

In recent years, market participants, including the GSEs, FHA, and the MBA, which represents certain market participants, have established loss mitigation standards to memorialize successful components of crisis-era programs or to encourage a degree of standardization for servicers across the private, federally supported, and federally insured mortgage markets. The GSEs' Flex Modification (FlexMod), implemented in 2017, closely aligns with MBA's One Modification

331. 31 U.S.C. § 3730(c)(2). Pursuant to a January 10, 2018 memorandum from Michael Granston, Director, Frauds Section of the Commercial Litigation Branch, DOJ attorneys have assessed whether declined qui tam cases are appropriate for dismissal.

proposal published in 2016.[332] Both the FlexMod and the MBA proposal reflect many of the lessons learned and standards adopted following the financial crisis. For example, both evaluate borrower hardship (short-term versus longer-term), offer solutions appropriate to that hardship that include retention and nonretention options, and aim to offer the most sustainable longer-term solution through the use of a waterfall of steps to achieve a modification that provides payment relief to the borrower and positive economic outcomes for the investor. Finally, FHA's loss mitigation program, which includes FHA-Home Affordable Modification Program (FHA-HAMP), shares many of the same features of the GSEs' present modification program, but utilizes different steps to achieve payment reduction.[333]

Despite agreement by most participants on the guiding themes for successful loss mitigation, the GSEs, FHA, VA, USDA, bank portfolio servicers, and private-label securities servicers continue to offer different loss mitigation programs. These differences are rooted in a number of underlying factors, including fundamental differences in the business models, regulatory and statutory mandates, and the borrower segments served by the range of private and federally-backed sources of mortgage financing. The main area in recent years where standardization and transparency has been achieved is across Fannie Mae and Freddie Mac with the implementation of their FlexMod – alignment facilitated by the GSEs' fundamentally similar business models and conservatorship under FHFA. FHA has a statutory mandate to hold capital and act as a fiduciary for the Mutual Mortgage Insurance Fund (MMIF).[334] Undertaking this fiduciary responsibility to the MMIF requires prompt liquidation of any assets assigned to it as a result of insurance claim payments (i.e., unlike the GSEs, FHA generally does not hold mortgage assets) — a program restriction that may constrain certain loss mitigation options.

Mortgage servicers cite the differences in loss mitigation programs as a particular challenge. Servicers, particularly specialty servicers who focus on delinquent and defaulted loans, will seldom service just one type of loan (e.g., all conventional or all government mortgages). Managing multiple standards limits efficiency and the ability to automate certain processes, restricts a servicer's ability to assess risk, and adds additional costs.

Furthermore, except for federal mortgage programs administered by FHA, VA, and USDA, a borrower does not necessarily know at origination whether his or her mortgage will be sold to a private credit investor or securitized through the GSEs — yet that same borrower faces two different experiences in the event of financial hardship that requires a loan workout solution. Borrowers, particularly during periods of hardship, benefit from clarity, and servicers benefit from certainty and scalability in terms of what assistance to offer a borrower who has experienced a hardship.

---

332. See Federal Housing Finance Agency, *Statement of FHFA Deputy Director Sandra Thompson on New Loan Modification Offering for Delinquent Borrowers* (Dec. 14, 2016), available at: *https://www.fhfa.gov/Media/PublicAffairs/Pages/Statement-of-FHFA-Deputy-Director-Sandra-Thompson-on-New-Loan-Mod-Offering-for-Delinquent-Borrowers.aspx*; see Mortgage Bankers Association, *Press Release – MBA Task Force Proposes Loan Modification Program to Provide At-Risk Homeowners Payment Relief* (Sept. 2016), available at: *https://www.mba.org/2016-press-releases/september/mba-task-force-proposes-loan-modification-program-to-provide-at-risk-homeowners-payment-relief*.

333. See HUD Mortgagee Letter 2009-23 and HUD Mortgagee Letter 2016-14.

334. 12 U.S.C. § 1708.

As such, mortgage loss mitigation is one part of the market that would benefit from a degree of alignment that does not presently exist.

Having a greater degree of standardization and transparency in place across the federal housing footprint would also accelerate the ability to respond in a future period of sustained market stress, as servicer, borrower, and mortgage investors would have procedures in place and an understanding of the exposures to more quickly administer loss mitigation solutions to struggling borrowers. Given the tendency of the housing market to exacerbate weakness during an economic downturn, having such a coordinated response in place could help mitigate the impact of housing market weakness on the broader economy.

In addition to potential benefits of greater alignment around loss mitigation programs, servicers have suggested a number of opportunities to increase efficiencies and reduce costs in FHA default servicing. Mortgage servicers believe that FHA servicing rules are complex and, in some cases, conflicting or outdated when compared to current industry practice reflected in GSE and PLS servicing and other regulatory requirements. Areas of potential enhancement include simplification of foreclosure timelines, restructuring of penalties associated with the failure to meet required timelines, and streamlining the foreclosed property conveyance process. These issues have been identified by HUD in its efforts to review and address needlessly burdensome and costly regulations.

Recommendations

Treasury recommends that federally supported mortgage programs explore standardizing the most effective features of a successful loss mitigation program across the federal footprint. Such standardization should broadly align a loss mitigation approach that facilitates effective and efficient loan modifications when in the financial interest of the borrower and investor, promotes transparency, reduces costs, and mitigates the impact of defaults on housing valuations during downturns. It should also establish parameters such as a standardized application package, affordability standards (e.g., suggested housing-expense-to-income ratios and minimum payment reductions), modification waterfall standards that specify suggested acceptable loss mitigation steps, and referral of delinquent borrowers to financial counseling. At the same time, these standards should not prescribe a specific modification product.

Additionally, Treasury recommends HUD continue to review FHA servicing practices with the intention to increase certainty and reduce needlessly costly and burdensome regulatory requirements, while fulfilling FHA's statutory obligation to the MMIF. In particular, Treasury recommends that FHA consider administrative changes to how penalties are assessed across FHA's multi-part foreclosure timeline to allow for greater flexibility for servicers to miss intermediate deadlines while adhering to the broader resolution timeline, as well as to better align with federal loss mitigation requirements now in place through the Bureau. Additionally, Treasury recommends FHA explore changes to its property conveyance framework to reduce costs and increase efficiencies by addressing frequent and costly delays associated with the current process. As an additional measure, Treasury recommends that FHA continue to make appropriate use of, and consider expanding, programs which reduce the need for foreclosed properties to be conveyed to HUD, such as Note Sales and FHA's Claim Without Conveyance of Title.

State Foreclosure Practices

Foreclosure practices are one of the most divergent state-level policies across the mortgage industry, and one for which certain housing markets have paid a high price in the decade since the housing market collapse. Foreclosure processes vary for each state but largely adhere to some combination of two formats: judicial and nonjudicial.

In a state with a requirement for a judicial review process, the owner of a mortgage note, typically the lender, is required to file a lawsuit in local court to foreclose on a defaulted borrower. Other states permit the lender to foreclose without going through the court system when a power of sale clause is present in the mortgage or deed of trust — a process referred to as a nonjudicial review. Some states allow both judicial and nonjudicial foreclosures but favor one or the other depending on the type of security instrument — mortgage or deed-of-trust — with judicial foreclosures more common with mortgages, and nonjudicial foreclosures with deeds-of-trust.

In states requiring judicial review, typically once the lender files a foreclosure lawsuit in court, the homeowner receives a summons and a copy of the foreclosure complaint. The homeowner can let the foreclosure proceed or contest it in court. If the homeowner chooses to contest, the court holds a hearing and a judge decides whether to let the foreclosure sale proceed and, if approved, sets an auction date. In states without a required judicial process, existing statutes establish the process required for a trustee to foreclose on a defaulted property. State law, and not the courts, determine the timeline and milestones in the foreclosure process. Some states have imposed additional required steps and remediation requirements regardless of judicial or nonjudicial review designed to afford additional protections to defaulted borrowers.

Since the financial crisis, foreclosure timelines have increased regardless of state foreclosure practices, with the national average timeline to complete a foreclosure climbing from approximately 6 months in 2007 to approximately 33 months by the end of 2017.[335] These timelines are generally considerably longer for those states that require judicial review.[336] While the national share of loans in the foreclosure process has returned to pre-crisis levels, the foreclosure rate in judicial review states remains elevated relative to both nonjudicial review states and the pre-crisis level,[337] with timelines in some judicial review states such as Florida and New Jersey exceeding 3 years on average.[338] In certain documented cases, borrowers in judicial review states have been able to remain in a property for over 5 years without making payments before a foreclosure is completed.[339]

---

335. ATTOM Data Solutions, *US Foreclosure Activity* (Apr. 2018), available at: *https://www.attomdata.com/news/market-trends/foreclosures/q1-2018-u-s-foreclosure-market-report/*.

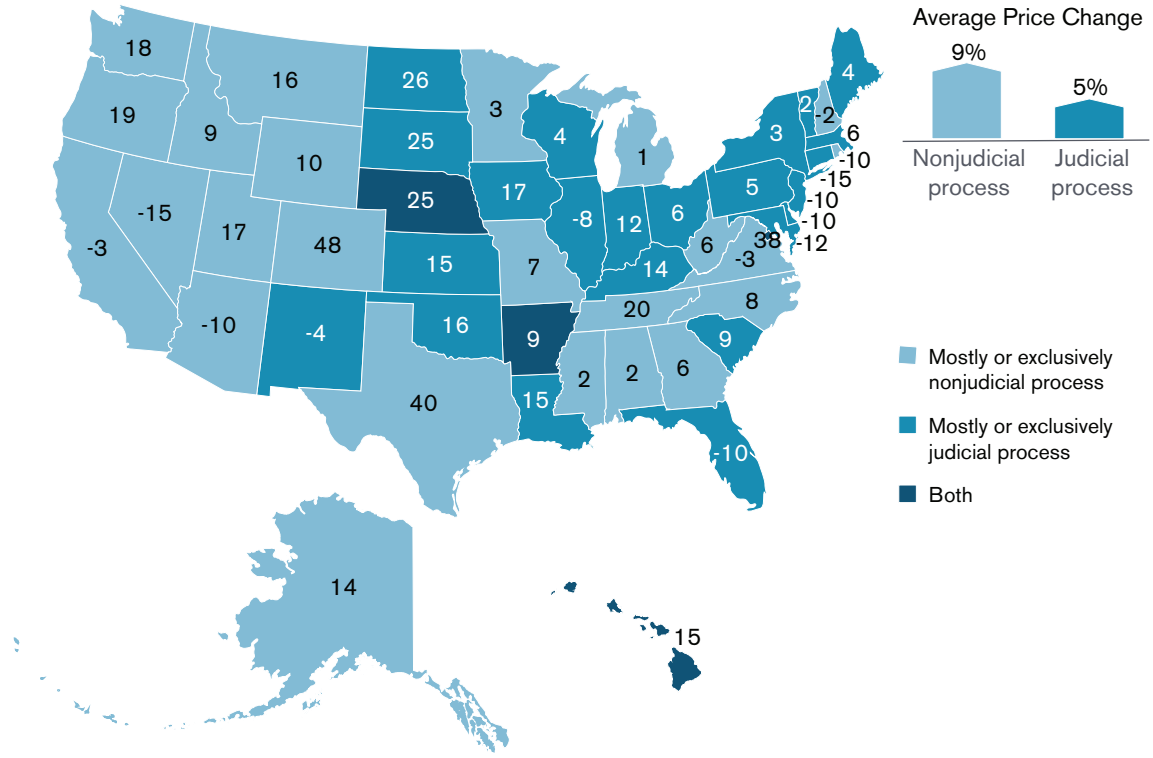
336. See Hamilton Fout et al., *Foreclosure Timelines and Housing Prices*, working paper (July 2017), available at: *http://www.fanniemae.com/resources/file/research/datanotes/pdf/foreclosure-timelines-and-house-prices-working-paper.pdf*.

337. Molly Boesel, CoreLogic*, Foreclosure Report Highlights: November 2016*, blog post (Jan. 10, 2017), available at: *https://www.corelogic.com/blog/2017/01/foreclosure-report-highlights-november-2016.aspx*.

338. See ATTOM Data Solutions.

339. Michael Corkery, *Homeowners Facing Foreclosure May Instead be Home Free,* Boston Globe (Mar. 30, 2015).

Figure 19: Foreclosure Process and Home Price Change Peak-to-Current by State (percent change)



Source: FHFA All Transactions Price Index, ATTOM Data Solutions Foreclosure Processes by State, and Treasury staff analysis.

Due to the high-cost of servicing nonperforming loans, borrowers in states with protracted foreclosure timelines will likely bear a portion of the cost of delays through a risk premium embedded in interest rates for loans made in that state.[340] Additionally, prolonged foreclosure timelines create a negative externality on home prices, which may harm nearby property values and dampen home price appreciation.[341] Since their pre-crisis peak, housing prices in states with a primarily nonjudicial review foreclosure process have appreciated twice as much as prices in states with a judicial review process.[342]

There is evidence that the judicial review foreclosure process leads to higher rates of persistent delinquency than nonjudicial review foreclosures, without measurably improving foreclosure

340. See Laurie Goodman, Urban Institute, *Servicing Costs and the Rise of the Squeaky-Clean Loan* (Feb. 2016), available at: *https://www.urban.org/sites/default/files/publication/77626/2000607-Servicing-Costs-and-the-Rise-of-the-Squeaky-Clean-Loan.pdf*.

341. See Eliot Anenberg and Edward Kung, *Estimates of the Size and Source of Price Declines due to Nearby Foreclosures*, 104 American Economic Review 2527–2551 (2014).

342. Treasury calculations based upon ATTOM Data Solutions foreclosure processes by state and FHFA Quarterly All-Transactions Home Price Index.

outcomes for borrowers.[343] Standardizing and moving away from a judicial review foreclosure process could reduce the time and resources involved in foreclosures and support home prices, without compromising borrower protections provided by federal and state regulation.

For federally supported housing programs that impose a degree of national pricing, such as the GSEs and FHA, some of the added cost from long foreclosure timelines is borne by borrowers in states with shorter timelines—effectively imposing a cross-subsidy from faster foreclosure states to slower ones. In response to state level differences in mortgage loss severities attributable to foreclosure process differences, the Federal Housing Finance Agency (FHFA) considered requiring the GSEs to impose an up-front fee in specific states where foreclosure costs exceeded the national average.[344] While FHFA elected not to pursue these charges, it did direct the GSEs in 2013 to maintain a quarter-point guaranty fee surcharge for four states — Connecticut, Florida, New Jersey, New York — where the foreclosure costs were more than two standard deviations above the national average.[345] All four states require judicial review foreclosure processes.[346] However, in January 2014, under a new director, FHFA reversed this decision and suspended any surcharge based on state foreclosure costs.[347]

Recommendations

Treasury recommends that states pursue the establishment of a model foreclosure law, or make any modifications they deem appropriate to an existing model law,[348] and amend their foreclosure statutes based on that model law. Treasury recommends federally supported housing programs, including those administered by FHA, USDA, VA, and the GSEs, explore imposing guaranty fee and insurance fee surcharges to account for added costs in states where foreclosure timelines significantly exceed the national average.

Nondepository Counterparty Transparency

Ginnie Mae guarantees the timely payment of principal and interest to investors in its securities, which are issued by lenders approved by Ginnie Mae and backed by government-guaranteed or insured mortgages. With the departure of credit investors in the wake of the housing collapse, Ginnie Mae experienced a surge in volume, as lenders and borrowers moved to access mortgage credit through government loan programs. Issuance of Ginnie Mae mortgage-backed securities (MBS) jumped from $97 billion in 2007 to $454 billion two years later, and has averaged over

343. See Kristopher Gerardi, Lauren Lambie-Hanson, and Paul S. Willen, *Do Borrower Rights Improve Borrower Outcomes? Evidence from the Foreclosure Process*, 73 J. of Urban Econ. 1 (2013).

344. See State-Level Guarantee Fee Pricing (Sept. 19, 2012) [77 Fed. Reg. 58991 (Sept. 25, 2012)].

345. See Federal Housing Finance Agency, *Press Release – FHFA Takes Further Steps to Advance Conservatorship Strategic Plan by Announcing an Increase in Guarantee Fees* (Dec. 9, 2013), available at: *https://www.fhfa.gov/Media/PublicAffairs/Pages/FHFA-Takes-Further-Steps-to-Advance-Conservatorship-Strategic-Plan-by-Announcing-an-Increase-in-Guarantee-Fees.aspx#*.

346. See ATTOM Data Solutions, *Foreclosure Laws and Procedures by State*, available at: *https://www.realtytrac.com/real-estate-guides/foreclosure-laws/* (last accessed June 15, 2018).

347. See FHFA Guarantee Fees History, available at: *https://www.fhfa.gov/PolicyProgramsResearch/Policy/Pages/Guarantee-Fees-History.aspx*.

348. See Uniform Law Commission, *Home Foreclosure Procedures Act* (2015), available at: *http://www.uniformlaws.org/Act.aspx?title=Home%20Foreclosure%20Procedures%20Act*.

$400 billion in the years since.[349] Between 2007 and 2017, the remaining principal balance of pools guaranteed by Ginnie Mae increased fourfold to $1.96 trillion.[350]

Ginnie Mae's issuer base has changed dramatically in both type and concentration, with nondepository issuers stepping into the market vacated by depositories exiting government loan programs. By the beginning of 2018, dedicated mortgage banks accounted for over 80% of Ginnie Mae issuance.[351] The GSEs, too, have seen their seller-servicer counterparty mix shift toward nondepositories, with nondepository lenders accounting for approximately half of the origination volume in 2017.[352] Market observers and participants, including Ginnie Mae, have asserted that the rapid increase in nondepository origination and servicing activity, combined with a less standardized approach to safety and soundness regulation, poses heightened counterparty risk. The disparity in banks and nonbanks prudential regulatory regimes has caused some market observers to question nonbank durability through the economic cycle and posit that nondepositories pose a systemic risk in general and a taxpayer risk in particular through the high share of nondepositories servicing Ginnie Mae pools.[353]

Nonbank servicers, like their bank competitors, are subject to a range of federal financial oversight. The Bureau, for example, supervises adherence to mortgage lending and servicing rules in addition to broader compliance with federal consumer financial laws. In addition, nondepositories are subject to oversight through counterparty minimum net worth, capital, and liquidity requirements imposed by the GSEs and Ginnie Mae.[354] As nonbanks are more dependent on execution through securitization, which at present is dominated by the GSEs and Ginnie Mae, compliance with GSE and Ginnie Mae counterparty requirements functions as an additional industry standard.

However, bank and nonbank lender-servicers face different safety and soundness regulatory standards. Insured depository institutions must abide by federal prudential regulation which includes standardized capital and liquidity regimes. Nondepositories are chartered and regulated at the state level and similarly face safety and soundness regulation, albeit by individual state banking examiners, despite the fact that these nondepositories may have a national footprint. While state regulators, facilitated by the Conference of State Bank Supervisors, have made progress in recent years toward developing more aligned standards for nonbank supervision, concerns about differing standards persist and have prompted calls for additional alignment.

---

349. See Ginnie Mae, *Monthly Issuance Reports – March 2018 Issuance Summary* (Apr. 13, 2018), available at: *https://www.ginniemae.gov/data_and_reports/reporting/Pages/monthly_issuance_reports.aspx*

350. See Ginnie Mae, *Monthly UPB Reports – March 2018* (Apr. 13, 2018), available at: *https://www.ginniemae.gov/data_and_reports/reporting/Pages/monthly_rpb_reports.aspx*.

351. See Urban Institute, *Housing Finance at a Glance* (May 2018), available at: *https://www.urban.org/research/publication/housing-finance-glance-monthly-chartbook-may-2018/view/full_report*.

352. Id.

353. See U.S. Government Accountability Office, *Nonbank Mortgage Services: Existing Regulatory Oversight Could Be Strengthened* (Mar. 2016), available at: *https://www.gao.gov/assets/680/675747.pdf*; Office of Inspector General, U.S. Department of Housing and Urban Development, *Ginnie Mae Did Not Adequately Respond to Changes in its Issuer Base* (Sept. 21, 2017), available at: *https://www.hudoig.gov/sites/default/files/documents/2017-KC-0008.pdf*.

354. See Fannie Mae, *Seller Guide* (June 5, 2018), at Part A4-1; Freddie Mac, *Seller/Servicer Guide* (June 13, 2018), at Chapter 2101; Ginnie Mae, *MBS Guide* (Jan. 25, 2018), at Chapter Three.

Furthermore, during periods of sustained financial stress, traditional depository lenders have access to sources of liquidity that nonbanks lack, such as insured customer deposits and FHLBs advances. Nondepositories are instead funded mainly through lines of credit and repurchase agreements, which, due to their short-term nature are subject to roll-over risk and margin requirements in the event of a deteriorating credit environment.[355]

High among concerns about nondepositories is the durability of these funding structures for nonbank servicers. When borrowers stop making mortgage payments, servicers of those loans continue to advance scheduled payments to investors and other parties until the delinquency has been resolved or the loan has been purchased out of its securitized pool. While servicers may be able to seek reimbursement for these advances depending upon the federal insurance or guaranty program, they must make them out of their own funds in the interim. Servicers of both GSE and Ginnie Mae securities face this risk; however, the higher delinquency rates and longer foreclosure timeline for FHA-insured loans underlying Ginnie Mae pools, as well as differences in delinquent loan buyout practices, may subject Ginnie Mae servicers to extended periods of liquidity strain exactly when financing may be most challenging. As counterparty risk represents Ginnie Mae's main financial exposure, its leadership is reasonably concerned with potential challenges from a sustained period of economic stress that tests the financial capacity of these nonbanks to continue to make servicing advances.

Ginnie Mae has multiple counterparty risk-management tools in use today, including on-site reviews, assignment of proprietary risk grades, and performance profiles. Additionally, Ginnie Mae, as well as the GSEs, have quarterly visibility into nonbank counterparty financial information, including debt facilities, through required submission of information through the Mortgage Bankers Financial Reporting Form.[356] However, data quality and the present fields required for reporting may be insufficient to provide the level of transparency needed to assess counterparty financial health. Ginnie Mae continues to pursue improvements to its counterparty risk management framework, including subjecting its servicers to a liquidity stress test to gauge the durability of their access to capital during a period of sustained financial stress.[357]

While the size of Ginnie Mae's portfolio and the nature of its counterparty risk has changed dramatically in recent years, Ginnie Mae lacks flexibility to adjust its MBS fees and hire additional staff to manage this risk. Under Ginnie Mae's charter, the maximum fee it can charge for its MBS guaranty is set at 6 basis points,[358] and is not permitted to be adjusted based on risks arising from changes in the housing market or from Ginnie Mae's counterparty exposure specifically. Additionally, Ginnie Mae's permanent staffing resources remain constrained, with approximately 150 permanent employees overseeing a $2 trillion portfolio. At present, Ginnie Mae depends on annual congressional appropriations to pay permanent staff. While Ginnie Mae is able to utilize its revenues to contract with outside firms for support services, stakeholders, including Ginnie

355. See Office of Financial Research, *Monitoring GNMA/GSE Pipeline Liquidity*, slide deck presentation (July 28, 2016), available at: *https://www.financialresearch.gov/frac/files/FRAC-meeting_GSE-Working-Group-Presentation_07-28-2016.pdf*.

356. See Fannie Mae Seller Guide, Freddie Mac Seller/Servicer Guide, and Ginnie Mae MBS Guide.

357. See Ginnie Mae 2020.

358. 12 U.S.C. § 1721(g)(3)(A).

Mae leadership, have highlighted the need for flexibility to hire permanent staff with the requisite experience, and compensated at competitive rates, to complement existing resources in providing risk management appropriate to oversee Ginnie Mae's considerable taxpayer exposure.[359]

Recommendations

Treasury recommends that Ginnie Mae collaborate with FHFA, the GSEs, and the Conference of State Bank Supervisors to expand and align standard, detailed reporting requirements on nonbank counterparty financial health, including terms and covenants associated with funding structures, to provide confidence that taxpayers are protected during a period of severe market stress. Additionally, Treasury supports Ginnie Mae's consideration of enhancing its counterparty risk mitigation approach, including through the imposition of stress testing requirements that can provide information on the financial health of servicer counterparties across an economic cycle. Furthermore, in order to protect taxpayers, Treasury recommends Ginnie Mae have sufficient flexibility to charge guaranty fees appropriate to cover additional risk arising from changes in the overall market or at the program level.

Treasury recommends a comprehensive assessment of Ginnie Mae's current staffing and contracting policies, including the costs and benefits of alternative pay and/or contracting structures. Ginnie Mae would be better equipped to manage its program and monitor counterparty risk if it were able to more readily attract personnel with requisite expertise by paying salaries comparable to those at other financial agencies with premium pay authority. Additionally, being able to adopt similar contracting procedures as other agencies that are outside of federal acquisition statutes and regulations would enable Ginnie Mae to more effectively monitor and respond to changing market conditions and needs. However, any change to Ginnie Mae's personnel or contracting policies should be informed by a comprehensive assessment of current challenges. The potential benefits of alternative pay and/or contracting structures should be weighed against the additional federal costs that would be incurred.

For nondepositories, providing greater transparency about their financial health should be a welcome step toward addressing concerns about their sustainability throughout the cycle and the risk they pose to taxpayers relative to their participation in federally supported loan and securitization programs. Furthermore, greater standardization of requirements and reporting could benefit nondepositories by reducing disparate state-level and principal counterparty requirements.

Student Lenders and Servicers

Overview

The majority of student loans are originated by the federal government through the U.S. Department of Education's (Education) Direct Loan Program. In 2010, Education fully moved to the Direct Loan Program, under which Education originates loans to students. At the same time, Congress ended a legacy guaranteed-loan program where private lenders were compensated by the

359. See HUD Office of Inspector General *Monitoring of Nonbank Issuers Presents Challenges for Ginnie Mae* (Mar. 13, 2017), available at: *https://www.hudoig.gov/reports-publications/topic-briefs/monitoring-of-nonbank-issuers-presents-challenges-ginnie-mae*.

federal government to originate and service federal student loans with guarantees of 97%. Today, the federal loan portfolio has nearly $1.4 trillion in outstanding student loans to nearly 43 million borrowers.[360] Federal student loan interest rates are set at a spread to the last 10-year Treasury note auction prior to June 1, with statutory caps by loan program. Federal student loans are originated at fixed rates. However, since interest rates fluctuate based on the interest rate on the relevant 10-year Treasury note, a student who has multiple loan types from multiple school years will have loans that carry different interest rates.

Figure 20: Federal Student Loan Interest Rates and Origination Fees

Loan Type	2017-18 Interest Rate	2018-19 Interest Rate	Statutory Interest Rate Cap	2017-18 Origination Fee
Subsidized Undergrad	4.45%*	5.05%	8.25%	1.066%
Unsubsidized Undergrad	4.45%	5.05%	8.25%	1.066%
Unsubsidized Graduate	6%	6.6%	9.5%	1.066%
Graduate PLUS	7%	7.6%	10.5%	4.264%
Parent PLUS	7%	7.6%	10.5%	4.264%

*Subsidized loans do not accrue interest while the borrower is in school and during a six-month grace period when the borrower leaves school.
Source: U.S. Department of Education and Treasury staff analysis.

Education provides both subsidized and unsubsidized loans to undergraduate borrowers, unsubsidized loans to graduate students, and higher interest loans with higher origination fees to both graduate and parent borrowers who do not have an adverse credit history. Undergraduate borrowers must comply with strict loan limits of $31,000 for dependent students and must demonstrate financial need. To manage repayment for the loans it has originated, Education hires and manages contractors who perform servicing and collections on the Direct Loan portfolio.

The private student loan market is small relative to the size of the federal portfolio at an estimated $113 billion, or about 8% of all outstanding student loans originated by banks, credit unions, and nonbanks.[361] The private student loan market also offers loans to undergraduates, graduate students, and parents but differs from the federal portfolio in that these loans are underwritten. The majority of private student loans are cosigned, with nearly all undergraduate loans in recent years requiring a cosigner; 92% in the 2017-18 award year, and 62% of graduate students requiring a cosigner in the same award year.[362]

In the past five years, more nonbanks have entered the student lending market with a focus on refinancing both private and federal loans into lower interest rate loans. While interest rates on

360. Office of Federal Student Aid, U.S. Department of Education, *Federal Student Aid Portfolio Summary*, available at: *https://studentaid.ed.gov/sa/about/data-center/student/portfolio* (as of the end of first quarter 2018) (last accessed June 15, 2018).

361. MeasureOne, *Private Student Loan Report – Q3 2017*, available at: *https://www.measureone.com/psl.php*.

362. Id. at 24.

these products may be lower than those on some federal student loans, the federal student loan program continues to provide borrower protections that are unmatched by private loan products. Federal student loan borrowers considering refinancing into private loans should carefully consider whether they will potentially utilize these federal benefits including: a variety of repayment plans including plans based on income, forbearances available for borrowers facing economic hardship, loan forgiveness programs after 20 or 25 years of income-driven repayments, Public Service Loan Forgiveness, and loan discharges for borrowers who become totally and permanently disabled.

Figure 21: Features of Federal Student Loans

	Description	Feature of Private Student Loans?	Feature of Other Consumer Credit Products?
Need based program	Federal student loans are not underwritten and instead are based on demonstrated financial need and in some cases cost of attendance.	No	No
Loan limits	Loan limits for undergraduate borrowers are based on whether borrower is considered "dependent" or "independent" not based on tax filing status but rather the borrowers age, marital status, military status, and children and other dependents.	No	No
Delayed repayment	Payment is not required while a borrower is in school or during a 6-month grace period after the borrower leaves school or drops below half-time enrollment.	Yes	No
Credit reporting	Delinquency on Direct Loans is not reported to the consumer credit bureaus until day 90 of delinquency.	No, delinquency reported begins as early as day 30.	No, all others report delinquency as early as day 30.
Late fees	Direct loans have no late fees	No	No
Interest capitalization	Interest capitalizes with every change in status on a federal student loan, including: entering repayment, leaving the grace period, switching repayment plans, use of deferments or forbearances, default, rehabilitating a defaulted loan, or consolidating existing loans. Interest capitalization increases the borrower's principal balance and interest expense paid over the life of the loan.	No	No
Interest accrual	Interest accrues on a daily basis, meaning the interest balance changes each day.	Yes	Daily interest accrual generally used in credit cards; monthly accrual is used in mortgages.
Repayment plans	Direct loans are eligible for up to eight repayment plans, some of which are dependent on eligibility requirements related to loan balance and date of loan origination. Some repayment plans cause negative amortization.	Generally only one amortizing repayment plan is offered.	No

Source: Treasury staff analysis.

Program Complexity and Impact

The federal student loan program is immensely complex due to: (1) the variety of loan types offered and outstanding legacy loan types that continue to require servicing; (2) eight repayment plans each with different eligibility requirements, repayment structures, and features; and (3) product features that differ from nearly all other consumer finance products. The natural consequence of this complexity is that it is difficult for borrowers, even those who are sophisticated, to navigate the program and effectively manage their repayment responsibilities. Because the program is difficult to understand, borrowers rely on servicers to answer questions about repayment, enroll borrowers in an appropriate and sustainable repayment plan, and assist borrowers when they struggle to make their payments. Federal student loan servicers have indicated to Treasury that the program's complexity not only makes loans more difficult to service, but also increases the cost of servicing. For example, call center staff at each federal student loan servicer must be well versed on all of the current and legacy loan types and repayment plans, as each have features with financial consequences and tradeoffs for borrowers.

Issues and Recommendations

Student Loan Servicing Standards

Due to the federal student loan program's complexity and Education's limited guidance on servicing standards, servicers have largely relied on internal business practices to determine how to effectively service federal student loans. While this was intended to promote innovation, it has caused difficulty for servicers in that (1) borrowers may be treated differently by different servicers, causing financial disparities, (2) Education's website provides generic information but each servicer must maintain its own website, (3) federal and state regulators have raised concerns with servicing practices, and (4) both the cost of servicing and difficulty of oversight have increased.

Borrowers in the same financial situation who contact two different servicers in the federal student loan program to enroll in a more affordable repayment plan may end up with different results and advice, which may result in a financial impact on the borrowers. Federal student loan servicers are instructed to enroll borrowers looking to reduce their payments into the plan that will cost the borrower the least over time. This sounds simple, but the servicer's call center agent may have only limited information from a borrower and may make decisions about tradeoffs between two similar repayment plans (e.g., Pay As You Earn and Revised Pay As You Earn) that confer slightly different benefits. Federal borrowers have also faced financial harm in even more straightforward circumstances, such as the application of over- and underpayments. Some servicers have not provided borrowers the ability to direct payments to a specific loan or have not fully implemented guidance from Education on how to process over- and underpayments.

Each servicer uses a proprietary format for its monthly statements and certain correspondence. Because of these disparities, Education's website lacks basic financial literacy information about how to read a monthly statement or plain language explanations of different letters sent by servicers with action steps on how to address the correspondence. To address this issue, servicers have created extensive proprietary websites aimed at serving their customers. Borrowers searching online for advice may get different information depending on their search results from Education's website and the servicer's website.

Federal student loan servicing currently lacks effective minimum servicing standards. This has created difficulties for federal student loan servicers when they communicate with regulators about their servicing practices. For example, a servicer may discuss a specific servicing practice with Education and gain approval for that practice but run into consumer protection concerns about the same practice in examinations or discussions with the Bureau. If Education prescribed minimum servicing standards, Education could vet these standards with other relevant agencies so servicers do not face conflicting guidance from multiple federal agencies. Further, a public, common servicing manual, like the servicing manual used in the federal guaranteed student loan program, would be helpful for state legislators and regulators considering additional regulation. With effective minimum servicing standards in place, states may decline to regulate federal student loan servicers further.

Finally, servicing standards could reduce the expense of servicing for taxpayers, as Education would not need to rely so heavily on contract change orders. In the current Direct Loan servicing contract, change orders are used to require servicers to take specific actions, for example to require servicers to conduct outreach to borrowers who must provide updated income information to remain in an income-driven repayment plan, but at a cost to the taxpayer. Servicing standards would reduce the need for these ad hoc contract changes, which are more expensive and difficult for servicers to implement than if built into the contract requirements up front. With common servicing standards, contract oversight would be easier for Education to conduct because both the servicer and Education would have clear, written guidance describing expectations.

Recommendations

Education should establish guidance on minimum standards specifying how servicers should handle decisions with significant financial implications (e.g., payment application across loans, prioritizing repayment plans, and use of deferment and forbearance options), minimum contact requirements, standard monthly statements, and timeframes for completing certain activities (e.g., processing forms or correcting specific account issues). Treasury applauds the required use of Education branding on servicing materials in the new Direct Loan servicing procurement to reduce borrower confusion.

Student Loan Borrower Communication

In the federal student loan program, servicers under contract with Education begin contacting borrowers directly following the disbursement of the borrower's first loan and will continue to contact the borrower at minimum on a quarterly basis while the borrower is in school and on a monthly basis while the borrower is in repayment. Federal student loan servicers rely heavily on U.S. mail, phone calls, and email to communicate with borrowers.

When loans enter repayment, borrowers generally create an online account with their student loan servicer. At this point, the servicer may receive the borrowers' email address for the first time as borrowers are not required to provide this information while applying for federal financial aid. Federal student loan servicers employ emails that many borrowers and consumer advocates feel are of limited utility as they often contain messages similar to, "A new message is available on your online account," rather than more substantive emails.

Federal student loan servicing also lacks e-signature capability, creating unnecessary cost and inefficiency for federal student loan servicers. Without e-signature, borrowers must access computers, find forms online, print physical copies of documents, sign those documents, then send those documents by mail, for processing and scanning in a servicer mail facility. This adds several steps for borrowers. To more successfully receive forms back from borrowers, some student loan servicers have mailed borrowers prepopulated forms and included an addressed and stamped envelope. The expense that servicers incur in using the U.S. mail for is significant relative to the monthly compensation federal student loan servicers receive per borrower. E-signature technology could expedite the process of completing forms and help borrowers more responsibly manage their student loan accounts, while reducing servicer costs. A reduction in servicer costs could also yield savings to the U.S. taxpayer in the form of lower servicer contract costs.

Recommendations

In Education's new Direct Loan servicing contract, Education should require student loan servicers to make greater use of emails and provide guidance to servicers on how to use email appropriately to balance privacy and security concerns with the need for effective and timely communication. All emails sent to federal student loan borrowers should provide enough information for borrowers to easily discern whether action must be taken on their account. Education should contract with providers of secure e-signature software and cloud technology for use by federal student loan servicers on all forms.

Data Quality

With a $1.4 trillion federal student loan portfolio, it is critical that Education monitor and manage the taxpayer investment in higher education carefully. Under the existing Direct Loan servicing contract, servicers maintain the majority of loan level data about the portfolio. Because data about the student loan portfolio comes from many different sources (e.g., borrowers, schools, legacy lenders and servicers, and nine current servicers), the data is often in incompatible formats and housed in separate, antiquated systems. This limits Education's ability to appropriately monitor trends in performance that should be addressed through servicing changes and manage the federal student loan portfolio. Further, Education releases very limited data about the performance of the portfolio. Taxpayers deserve greater insight into how this large investment is performing.

Recommendations

Education must improve its data quality and portfolio management. Education's Office of Federal Student Aid, which operationalizes the $1.4 trillion federal student loan portfolio, should include in its management team individuals with significant expertise in managing large consumer loan portfolios.

Education should take steps to address existing data quality issues to better monitor and manage portfolio performance. Education should increase transparency by publishing greater portfolio performance data, servicer performance data, and cost estimation analysis on its website to give stakeholders greater insight into Education's management of the taxpayer investment in higher education.

Institutional Accountability

Treasury remains concerned about the lack of institutional accountability in student lending. Colleges and universities have very few accountability requirements related to the performance of the loans their students receive through the federal student loan program. The existing metric used by Education, the cohort default rate, does not capture other problematic loan statuses that show the borrower may be struggling to repay (e.g., significant delinquencies and extended forbearances) and the metric is easily gamed by institutions. Treasury analysis of Education data indicates that principal repayment after five years is highly predictive of future loan performance. Treasury is concerned about schools that do not provide student loan borrowers good value, often leading to indebtedness the borrower cannot repay in a reasonable time period.

Recommendations

Treasury supports legislative efforts to implement a risk-sharing program for institutions participating in the federal student loan program based on the amount of principal repaid following five years of payments. Schools whose students have systematically low loan repayment rates should be required to repay small amounts of federal dollars to protect taxpayers' growing investment in the federal student loan program. Congress should consider how to address schools with systematically low repayment rates but large populations of disadvantaged students.

Short-Term, Small-Dollar Installment Lending

Overview

Short-term, small-dollar loans, which typically range from $300 to $5,000, account for nearly $90 billion in annual lending.[363] These products, offered by nonbank lenders and some depository institutions, include lump-sum loans, with terms of 1 month or less, as well as installment loans with terms of up to 2 years. The demand for short-term, small-dollar products is high because many households struggle with income volatility, thin or no credit files or a subprime score, or lack of access to mainstream financial products that meet their needs. According to the FRB, 40% of Americans say they could not easily cover an emergency expense of $400.[364] FDIC data also indicates that almost 20% of U.S. households are considered underbanked because of their use of alternative financial services.[365]

---

363. See Center for Financial Services Innovation, *2017 Financially Underserved Market Size Study* (Dec. 2017), at 44–47, available at: *https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2017/04/27001546/2017-Market-Size-Report_FINAL_4.pdf* (for revenue and volume data on pawn loans, online payday loans, storefront payday loans, installment loans, title loans, and marketplace personal loans).

364. Board of Governors of the Federal Reserve System, *Report on the Economic Well-Being of U.S. Households in 2017* (May 2018), at 21-22, available at: *https://www.federalreserve.gov/publications/files/2017-report-economic-well-being-us-households-201805.pdf*.
Board of Governors of the Federal Reserve System, *Report on the Economic Well-Being of U.S. Households in 2016* (May 2017), at 26-27, available at: *https://www.federalreserve.gov/publications/files/2016-report-economic-well-being-us-households-201705.pdf*.

365. Federal Deposit Insurance Corporation, *2015 FDIC National Survey of Unbanked and Underbanked Households* (Oct. 20, 2016), available at: *https://www.fdic.gov/householdsurvey/*.

Regulatory Framework Regulatory Framework

Nonbank, short-term, small-dollar lenders are regulated at both the federal and state levels. At the federal level, Dodd-Frank authorized the Bureau to supervise nondepository covered persons offering or providing payday loans to consumers for compliance with federal consumer protection laws.[366] As noted previously, the Bureau also has authority to prohibit certain acts or practices that are unfair, deceptive, or abusive.

State laws set product feature limitations and may require licensing of nonbank lenders to make loans in the state. Based on the product (e.g., payday or installment), product feature restrictions may include loan size caps, interest rate limits, repetitive use restrictions, and even outright prohibitions. These restrictions are often enforced by state banking agencies or state attorneys general. According to the National Conference of State Legislatures, 37 states have laws allowing payday lending in some form. Thirteen states have prohibited payday lending outright.

Banks providing short-term, small-dollar loans may be regulated by state or federal law, depending on the type of bank. Prudential regulators and the Bureau have authority to evaluate these product offerings for compliance with federal consumer protection laws. Additionally, as depository institutions, banks offering these products must meet safety and soundness requirements.

Issues and Recommendations

In November 2017, the Bureau issued a final rule entitled "Payday, Vehicle Title, and Certain High Cost Loans" (Payday Rule) that applies to lenders that extend credit with terms of 45 days or less as well as longer-term credit with balloon payments (Covered Loans).[367] Lenders making Covered Loans are required to determine that the borrower has the ability to repay the loan. This ability to repay is based on a determination that the consumer can make payments on the loan and still meet major financial obligations and basic living expenses without needing to re-borrow over the next 30 days. When underwriting a Covered Loan, the lender is required to obtain and verify the consumer's net income and financial obligations and ensure that the loan will not result in the consumer having a sequence of more than three Covered Loans within 30 days of each other. A failure to comply with the ability to repay underwriting standard is an unfair and/or abusive practice. In January 2018, the Bureau announced its intention to engage in further rulemaking to reconsider the Payday Rule.

The Bureau's rule raises two primary concerns. First, states maintain authority to regulate short-term, small-dollar lending, which raises questions regarding the need for additional federal regulation. In 2016, the House Financial Services Committee held a hearing to evaluate the Bureau's proposed Payday Rule and its interaction with state authority. Testimony highlighted the extensive action taken by states to pass laws authorizing, restricting or prohibiting payday lending. Similarly, in 2016, a bipartisan group of 16 state attorneys general sent a letter to then Bureau Director Cordray cautioning him against restricting state authorities by moving forward with the Payday Rule. Specifically, these attorneys general highlighted how states were best positioned to regulate

366. 12 U.S.C. § 5514(a)(1)(E).

367. Payday, Vehicle Title, and Certain High-Cost Installment Loans (Oct. 5, 2017) [82 Fed. Reg. 54472 (Nov. 17, 2017)].

these sometimes high-priced products, and to understand the credit and consumer protection needs of the consumers in their states.

Second, the Payday Rule would further restrict consumer access to credit and decrease product choices. According to the Bureau's estimates, the Payday Rule would reduce overall payday loan volume by as much as two-thirds.[368] This reduction in access to regulated, short-term, small-dollar loans may leave these consumers vulnerable to dangerous alternatives such as unscrupulous, unlicensed, offshore or otherwise illegal lenders.[369] This is especially true as short-term, small-dollar lending activity has been largely pushed out of the traditional banking system.

Banks can operate as additional sources of credit for consumers who otherwise may be unbanked or underbanked and lead to "a path to more mainstream financial products."[370] However, in 2013, the OCC and FDIC issued guidance on direct deposit advance products, which identified supervisory risks with the offering of these products.[371] Following the release of the guidance, banks withdrew these products from the market. Stakeholder feedback highlighted that the low margin and heightened maintenance of these products did not offset the increased regulatory scrutiny. This outcome further restricted short-term, small-dollar lending from the traditional banking system.

Last year, the OCC recognized the consumer demand for these products. In October 2017, the OCC rescinded its guidance because "consumers who would prefer to rely on banks and thrifts for these products may be forced to rely on less regulated lenders and be exposed to the risk of consumer harm and expense."[372] The OCC has also issued a bulletin providing guidance to OCC-supervised banks on core lending principles for short-term, small-dollar installment lending.[373] The FDIC has yet to rescind its previous guidance.

Recommendations

Treasury recognizes and supports the broad authority of states that have established comprehensive product restrictions and licensing requirements on nonbank short-term, small-dollar installment lenders and their products. As a result, Treasury believes additional federal regulation is unnecessary and recommends the Bureau rescind its Payday Rule.

Additionally, Treasury recommends that federal and state financial regulators take steps to encourage sustainable and responsible short-term, small-dollar installment lending by banks. Specifically,

---

368. Id. at 54817.

369. Sudhir Venkatesh, Off the Books: The Underground Economy of the Urban Poor (2006); Todd J. Zywicki, Mercatus Center, *The Case Against New Restrictions on Payday Lending*, working paper (July 2009), available at: *https://www.mercatus.org/system/files/WP0928_Payday-Lending.pdf*.

370. Office of the Comptroller of the Currency, *Core Lending Principles for Short-Term, Small-Dollar Installment Lending*, OCC Bulletin 2018-14 (May 23, 2018), available at: *https://www.occ.treas.gov/news-issuances/bulletins/2018/bulletin-2018-14.html* ("OCC Core Lending Principles").

371. Direct Deposit Advance products, offered by banks, are a "small-dollar, short-term loan or line of credit that a bank makes available to a customer whose deposit account reflects recurring direct deposits." Rescission of Guidance on Supervisory Concerns and Expectations Regarding Deposit Advance Products (Oct. 5, 2017) [82 Fed. Reg. 47602 (Oct. 12, 2017)].

372. Id.

373. OCC Core Lending Principles.

Treasury recommends that the FDIC reconsider its guidance on direct deposit advance services and issue new guidance similar to the OCC's core lending principles for short-term, small-dollar installment lending.

Debt Collection

Debt collectors and debt buyers are important market participants for the continued functioning of the consumer credit markets and other industries that rely on the recoveries from debt collection or the sale of delinquent debt to minimize losses.[374] Debt collectors can be segmented into two categories: first-party debt collectors and third-party debt collectors. By reducing losses from unpaid balances, debt collectors and debt buyers increase efficiency in the consumer credit markets through the reduced cost of credit, which can yield greater access to credit.

Issues and Recommendations

The Fair Debt Collection Practices Act (FDCPA), was enacted in 1977 to eliminate abusive, deceptive, and unfair conduct by third-party debt collectors working to collect consumer debt incurred primarily for personal, family, or household purposes, thereby excluding business, corporate, or agricultural debt.[375] Dodd-Frank provided the Bureau rulemaking authority for the FDCPA, as well as supervision and enforcement authority for the entities under the Bureau's jurisdiction.[376] The Bureau's supervision manual for the FDCPA makes clear that an institution is not considered a debt collector under the FDCPA, "when it collects: another's debts in isolated instances; its own debts it originated under its own name; debts it originated and then sold, but continues to service (e.g., mortgage and student loans); debts that were not in default when they were obtained; and debts that were obtained as security for a commercial credit transaction."[377] These exclusions from the FDCPA allow creditors who have originated the debt (first-party debt collectors) to attempt recovery on that debt without the restrictions and potential liability associated with the FDCPA.

Debt collectors and debt buyers are of continued interest to policymakers, as they are frequently the source of consumer complaints and yielded one of the most frequent types of consumer complaints of any industry to both the Federal Trade Commission (FTC)[378] and the Bureau[379] in the

374. The majority of debt collected is related to healthcare, student loans, and debt owed to state, local, and federal governments. See Ernst & Young, *The Impact of Third-Party Debt Collection on the US National and State Economies in 2016* (Nov. 2017), at 5, available at: *https://www.acainternational.org/assets/ernst-young/ey-2017-aca-state-of-the-industry-report-final-5.pdf*.

375. Bureau of Consumer Financial Protection, *Fair Debt Collection Practices Act Supervision Manual* (Oct. 2012), available at: *https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102012_cfpb_fair-debt-collections-practices-act-fdcpa_procedures.pdf* ("FDCPA Supervision Manual").

376. Dodd-Frank §§ 1002(12)(H), 1024(b)-(c), and 1025(b)-(c) [12 U.S.C.§§ 5481(12)(H), 5514(c), and 5515(c)].

377. FDCPA Supervision Manual, at 1.

378. Federal Trade Commission, *Consumer Sentinel Network Data Book 2017* (Mar. 2018), at 4, available at: *https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf*.

379. Bureau data from Consumer Complaint Database, available at: *https://www.consumerfinance.gov/data-research/consumer-complaints/* (filtered for complaints received during 2017).

last year. Stakeholders representing a variety of interests, including consumer advocates, lenders, debt collectors and debt buyers, and the FTC, have expressed concerns about the adequacy of information transferred with the sale of debt to third-party debt collectors. Data provided by industry indicates there is an inefficiency in this market as well. According to a survey of debt collectors and buyers, consumers request verification on nearly one in five accounts referred to debt collectors, with approximately 10% of consumers filing a formal dispute.[380] While FTC data shows fewer disputes, the FTC reports that debt buyers indicate they are only able to verify about half of the debts that consumers dispute, demonstrating that debt buyers are not receiving sufficient information about the debt to prove to the consumer that the debt they are attempting to collect is valid.[381]

In 2013, the Bureau published an advance notice of proposed rulemaking on debt collection practices.[382] In the proposal, the Bureau indicated concern about the amount of information that is transferred with a debt when it is sold to a third-party collector, and requested comment on what type of information should be provided in three critical areas and the adequacy of that information: (1) the correct person; (2) the correct amount owed; and (3) the correct documentation provided with the debt.[383] To date, the Bureau has not issued a notice of proposed rulemaking following the 2013 proposal. In the absence of minimum federal standards for the information creditors must provide to debt collectors and buyers, certain companies and trade groups have committed to higher standards for this information prior to debt collection or sale. Additionally, some states have enacted laws concerning data quality standards for debt buyers and required disclosures. For example, California law prohibits debt buyers from contacting consumers about a debt unless it possesses information about the debt balance, date of default, and original creditor. Illinois, Texas, and New York statutes require disclosure of specific information to consumers by debt collectors.

Recommendation

Treasury recommends the Bureau establish minimum effective federal standards governing the collection of debt by third-party debt collectors. Specifically, these standards should address the information that is transferred with a debt for purposes of debt collection or in a sale of the debt. Further, the Bureau should determine whether the existing FDCPA standards for validation letters to consumers should be expanded to help the consumer assess whether the debt is owed and determine an appropriate response to collection attempts.

Treasury does not support broad expansion of the FDCPA to first-party debt collectors absent further Congressional consideration of such action.

---

380. Ernst and Young, at 5.

381. Federal Trade Commission, *The Structure and Practices of the Debt Buying Industry* (Jan. 2013), at iv, available at: *https://www.ftc.gov/sites/default/files/documents/reports/structure-and-practices-debt-buying-industry/debtbuyingreport.pdf*.

382. Debt Collection (Regulation F) (Nov. 5, 2013) [78 Fed. Reg. 67848 (Nov. 12, 2013)].

383. Id.

IRS Income Verification

Overview

The federal government plays a role not only supporting policies that advance the prudent application of financial technology in credit markets, but also, at times, by furnishing information integral to the consumer and small business underwriting process itself. In this capacity, the government needs to take care that it is not inhibiting innovation in practice that it supports in policy. One commonly cited credit industry challenge is the interaction with IRS's income verification system, including the lack of an interface, such as an Application Programming Interface (API), to perform this function in an automated fashion.

As part of assessing a loan applicant's financial capacity for assuming a credit obligation, lenders for consumer and small business credit often request that a loan applicant provide tax return information to verify income information submitted by the applicant. For some credit decisions, such as mortgages, lenders perform income verification to adhere to regulatory requirements to assess a borrower's ability to repay the debt. For other classes of credit, particularly those served by marketplace lenders, income verification is an important credit risk assessment tool as it helps develop a more complete picture of a borrower's overall risk assessment and the likelihood for that borrower to be able to fulfill the terms of the loan.[384]

Lenders assess financial capacity using a range of information and tools. Some information is provided directly by the borrower. Other information is provided by third parties, some of which requires the consent of the borrower before such information can be provided to the lender. For credit decisions, loan terms are largely determined by applicant-submitted information and data purchased from private credit bureaus that document the credit histories of millions of Americans. Official tax return documentation obtained pursuant to authorization provided by the borrower is a critical source of information and is used by lenders to verify that loans comply with existing regulations (e.g., the Ability to Repay/Qualified Mortgage rule) and to confirm information provided by the borrower during the underwriting process. Lenders generally determine a borrower's creditworthiness before utilizing official income data, due in part to challenges with quickly and securely obtaining tax return information from the IRS once the borrower authorizes the IRS to disclose such information to the lender.

Issues and Recommendations

In the present system, a credit applicant facilitates income verification by completing a request for a copy of his or her tax transcripts through IRS Forms 4506, 4506-T, 4506T-EZ, or 8821 through the IRS.[385] Through these forms, a borrower gives consent for the IRS to disclose his or her summarized tax transcript to a third party.[386] Lenders often utilize third-party vendors to process these

384. See Marketplace Lending Association, *Update the IRS 4506-T API*, available at: *http://marketplacelendingassociation.org/wp-content/uploads/2017/08/Build-an-API-for-the-IRS-4506-T-.pdf*.

385. See IRS Income Verification Express Service at *https://www.irs.gov/individuals/international-taxpayers/income-verification-express-service*.

386. Federal law prohibits disclosure or use of federal tax return information except as authorized by that title. See 26 U.S.C. § 6103. Violations are subject to criminal penalty. Federal law [26 U.S.C. §6103(c)] permits the IRS to disclose tax return information to third parties with consent of the taxpayer.

transcript requests. To protect the confidentiality of federal tax return information, third-party vendors must meet strict security and technology requirements set by the IRS.

The IRS typically processes transcript requests submitted through its Income Verification Express Service and provides borrower tax summary data to the authorized third party within two to three days, although lenders report it can take considerably longer during periods of high volume. Credit decisions can be delayed pending receipt. Given the millions of credit transactions that depend on IRS verification, delays in this process may impose added costs on borrowers and the economy from the collective delays in completing these transactions. In a financial system increasingly adopting real-time information transfer and access to borrower bank and asset profiles, the delay in receiving IRS income verification can be particularly frustrating for lenders and borrowers.

The IRS currently fulfills 4506-T requests by transmitting borrower tax summary data to an authorized third party's secure mailbox. In other data aggregation situations, such as gathering borrower bank balances, lenders are able to obtain the needed borrower financial information through an API to instantaneously and safely transfer data. However, for lenders to gather federal tax data, they must rely on slower IRS verification technology that lacks the key type of digital interface enabled by an API. Given existing IRS priorities and funding levels, developing such a digital interface capability at the IRS would require multiple levels of front-end as well as back-end enhancements, including development of an e-signature capability and an authorization solution.

Enabling faster, more reliable income verification could facilitate lenders' ability to better incorporate historical income data earlier into credit pricing, as opposed to using it for verification purposes at the back-end of the underwriting process. Further, this data could potentially expand access to credit by providing lenders a broader view into a credit applicant's creditworthiness, where an otherwise incomplete credit picture, or on-the-border credit score, could lead a lender to decline an applicant. This is particularly true for small businesses, as it could improve the ability to consolidate debts incurred on personal credit cards into a consolidated business loan, as a lender would be able to more immediately analyze income history and observe patterns of growth that indicate creditworthiness.

Recommendation

It is important that the IRS update its income verification system to leverage a modern, technology-driven interface that protects taxpayer information and enables automated and secure data sharing with lenders or designated third parties. Such an interface would bring a critical component of the credit process up to speed with broader innovations in financial technology. Borrowers, and the broader economy, stand to benefit through lower operational costs for lenders, elimination of paperwork and delays, incorporation of important credit information into credit pricing, and potentially expanded access to credit as tax information can be more easily incorporated into determinations of creditworthiness. Any changes must balance faster access with security controls that ensure that only information that borrowers choose to share with lenders is shared, that lenders and vendors have security controls in place to protect taxpayer data, and that significant security protections are put into place to protect sensitive taxpayer information.

While the IRS is working to update its technology, including technology used by lenders for income verification, these efforts are dependent on funding in light of other IRS mission-critical priorities.

Treasury recommends Congress fund IRS modernization, which would include upgrades that will support more efficient income verification.

New Credit Models and Data

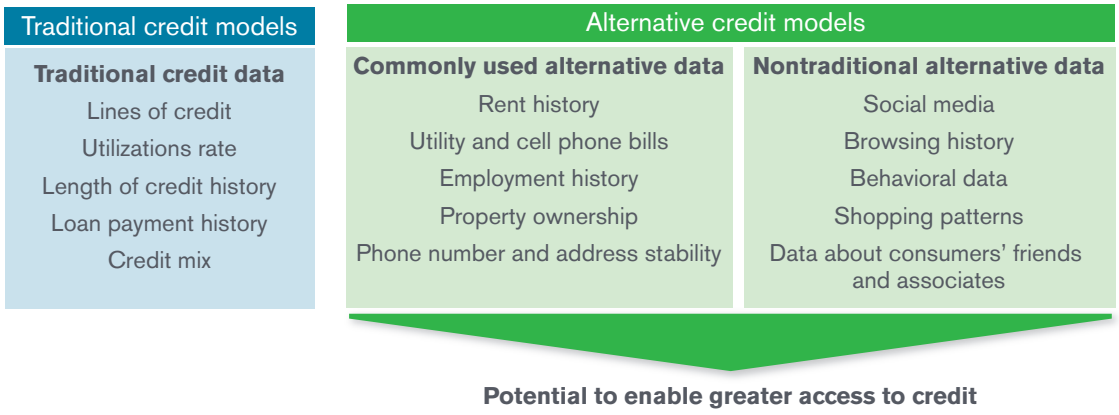
Overview

U.S. financial institutions have traditionally relied upon a common set of credit information for purposes of extending consumer credit. This generally standardized credit data, which consists primarily of consumer debt and payment history, is consolidated by national credit bureaus and is fed into a common set of credit models which generate consumer credit scores that are widely used across U.S. financial institutions. One of the most dominant existing credit score models is the one used by FICO to generate the widely used FICO score, which is reportedly used by some 90% of top lenders.[387]

With the explosion in available data and advances in modeling methods, a growing number of firms — existing and new entrants — have begun to use or explore a wide range of newer data sets or advanced algorithms (including those based upon machine-learning practices) to support credit underwriting decisions. This interest in newer data and models has taken place across the unsecured consumer, small business lending, and mortgage lending segments.

The types of data being considered may differ significantly in their apparent relationship to traditional credit criteria. Some data are considered more proximate because they provide more meaningful information on the credit profile of borrowers (e.g., utility and rental payments), while

Figure 22: Types of Credit Data



Note: Represents select examples from comment letters to CFPB regarding use of alternative data and modeling technologies in credit process by Equifax, TransUnion, American Bankers Association, Consumer Bankers Association, FICO, Independent Community Bankers Association, and California Nevada Credit Union League.
Source: CFPB public comment file. See Robinson + Yu, *Knowing the Score: New Data, Underwriting, and Marketing in the Consumer Credit Marketplace* (Oct. 29, 2014), at 15.

387. See Mercator Advisory Group, *Press Release – FICO® Scores Used in over 90% of Lending Decisions According to New Study* (Feb. 27, 2018), available at: *http://paymentsjournal.com/fico-scores-used-90-lending-decisions-according-new-study/*.

other data sources' relationship to credit risk may be less apparent (e.g., technology usage patterns, social networking information and website tracking).

The types of credit models also vary meaningfully, for example, by the degree to which firms employ machine learning based algorithms. Some of the new credit models are largely based upon existing modeling approaches but with new forms of data that closely approximate other credit data, while other firms may employ both new modeling approaches (i.e., machine learning) and some of the newest forms of data (e.g., technology use patterns). These newer credit models could be used by firms on a proprietary basis to underwrite borrowers for their own businesses, or could also be used by firms to generate a credit score product that could be sold to other firms for their loan underwriting processes.

Nonbank financial firms, such as marketplace lenders, generally report greater use of less-traditional data sources and newer modeling approaches, including ones based upon machine learning. Such lenders may rely upon new data sources to support the underwriting of loans through authenticating borrowers' identity online, assessing borrower default risk, and reducing instances of fraud. The provision of such scoring information also allows such lenders to often extend credit to borrowers below traditional FICO score thresholds or with little FICO score information.[388] Various new credit scoring companies have also formed that are generally more active in leveraging these new data sources, though the degree to which some might employ machine-learning models can vary substantially.[389]

Issues and Recommendations

These approaches have the potential to enable greater access to credit and improve the quality of financial products. However, the applications of these more novel approaches raise important policy considerations.

Opportunities to Expand and Improve Access to Credit

There are potential opportunities to expand access to credit for borrowers: (1) consumers who have thin credit files or no credit files (up to 45 million U.S. adults)[390] with the consumer credit bureaus, and (2) small businesses, which are important engines of the economy and job creation. For example, a 2017 study found some evidence that the use of "alternative" credit data has allowed consumers with more limited traditional credit profiles (i.e., based on FICO scores) to access credit.[391] Additional information on credit card usage, such as whether consumers are carrying balances

388. See Letter from the Online Lenders Alliance to the Bureau of Consumer Financial Protection, *Response to Request for Information Regarding Use of Alternative Data Modeling Techniques in the Credit Process; Records Docket No.: CFPB-2017-0005* (May 19, 2017), available at: *https://www.regulations.gov/document?D=CFPB-2017-0005-0071*.

389. Mikella Hurly and Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 Yale J. L. & Tech. 148 (2016) (table 1).

390. See Office of Research, Bureau of Consumer Financial Protection, *Data Point: Credit Invisibles* (May 2015), at 12, available at: *http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf* ("Credit Invisibles Report").

391. Julapa Jagtiani and Catharine Lemieux, *Fintech Lending: Financial Inclusion, Risk Pricing, and Alternative Information*, Federal Reserve Bank of Philadelphia working paper (July 6, 2017), at 9-12, available at: *https://www.philadelphiafed.org/-/media/research-and-data/publications/working-papers/2017/wp17-17.pdf*.

month over month on their credit cards or paying in full, can also improve credit risk analysis. At the same time, some groups have raised the concern that expanding the use of certain data (e.g., rent, utility, telecom payments) for persons that already have a FICO score could result in reduced credit availability.[392] The use of alternative credit data can provide consumers an on-ramp into the financial services landscape. For example, FICO recently launched another credit score product designed to provide credit applicants a "second chance" score, to be used where the applicant has no traditional FICO score. The new score provides a means to assess consumers with thin credit reports who could not be scored without additional information. FICO found that using its "second chance" score, more than a third of such applicants had FICO scores above 620. Moreover, for applicants with scores above 620 and that access credit, more than two-thirds reported FICO scores of 660 or higher two years later.[393]

Several firms that are actively deploying these approaches in consumer and small business lending report significant improvements in loss rates, which suggests some improvements in modeling approaches. For example, firms anecdotally report: (1) double-digit improvements in approval rates and declines in loss rates from using machine learning techniques on existing available data sources for lenders (that is, their own data, but with improved analysis); and (2) that some of the nontraditional data sources provide predictive value that is comparable to the traditional credit-data, which can indicate either strong proxy relationships with traditional credit-data or other important information not available to existing credit data sets. It should be noted, however, that the timeframe of these favorable results is limited and does not reflect performance through a credit cycle.

The Bureau has also highlighted the potential benefits in these approaches to data and modeling. The Bureau launched a no-action letter program as part of its Project Catalyst, launched in November 2012, to facilitate consumer-friendly innovations. Specifically, the Bureau was looking to explore how "alternative data" and the use of emerging technologies like machine learning, could improve credit decisions.[394]

Consumer Protections and Compliance

Firms looking to use alternative data and more advanced algorithms must navigate compliance with several areas of consumer protection law, including: (1) the Fair Credit Reporting Act (FCRA) of 1970, which is designed to make sure that credit reporting agencies that sell data for certain decision-making purposes maintain accurate data, provide consumers access to and the ability to correct their data, and that such data is used only for permissible activities; (2) fair lending laws, including the Equal Credit Opportunity Act and the Fair Housing Act, which are

392. Letter from National Consumer Law Center et al., *Comments in Response to Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process, Docket No. CFPB-2017-0005* (May 19, 2017), at 3-4, available at: *https://www.regulations.gov/document?D=CFPB-2017-0005-0097*.

393. Letter from Fair Isaac Corporation, *Request for Information Regarding the Use of Alternative Data and Modeling Techniques in the Credit Process – Docket No. CFPB-2017-0005* (May 19, 2017), at 9, available at: *https://www.regulations.gov/document?D=CFPB-2017-0005-0080*.

394. Bureau of Consumer Financial Protection, CFPB Announces First No-Action Letter to Upstart Network (Sept. 14, 2017), available at: *https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-first-no-action-letter-upstart-network/*.

designed to prohibit discrimination on the basis of various protected categories; (3) the Federal Trade Commission (FTC) Act, which prohibits unfair or deceptive acts or practices (UDAP) in or affecting commerce; and (4) the Bureau's authority with respect to unfair, deceptive or abusive acts and practices (UDAAP).

The FCRA requires that consumers be provided adverse action notices if they are denied credit or charged more as the result of their consumer report information. This requirement, among other factors, may represent challenges for market participants that are seeking to innovate by incorporating additional data sources into the credit underwriting process.

New models and data may also unintentionally run the risk of producing results that arguably risk violating fair-lending laws if they result in a "disparate impact" on a protected class[395] or because the FTC or the Bureau might find the use of such models and data to be a violation of UDAP or UDAAP, respectively.

Model Validation and Reliability

Existing regulatory guidance on credit models[396] may need to be tailored to incorporate issues raised by alternative data or machine learning based models. As an example, applying traditionally accepted practices of model validation and back-testing may be challenging when models are constantly "learning" and producing potentially new results on a continual basis.

The data available today significantly exceeds the data available during past credit cycles. Machine learning based models that require significant amounts of data would generally suffer from the absence of past credit-cycle data to "train" the model.

Data Quality and Privacy

Alternative data sources may not be as reliable as traditional sources. Banks active in consumer lending, for example, report that vendors of "alternative data" may not always know the source of their own data, which would present material compliance risks if such data were to be used for

395. Carol Evans, Board of Governors of the Federal Reserve System, *Keeping Fintech Fair: Thinking about Fair Lending and UDAP Risks*, Consumer Compliance Outlook (2017), available at: *https://consumercomplianceoutlook.org/assets/2017/second-issue/ccoi22017.pdf?la=en*.

396. See Board of Governors of the Federal Reserve System, Guidance on Model Risk Management, SR Letter 11-7 (Apr. 4, 2011), available at: *https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm*; Office of the Comptroller of the Currency, Credit Scoring Models, OCC Bulletin 1997-24 (May 20, 1997), available at: *https://www.occ.treas.gov/news-issuances/bulletins/1997/bulletin-1997-24.html*; Office of the Comptroller of the Currency, Sound Practices for Model Risk Management, OCC Bulletin 2011-12 (Apr. 4, 2011), available at: *https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12.html*; Federal Deposit Insurance Corporation, Supervisory Insights – Model Governance (last updated Dec. 5, 2005, available at: *https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin05/article01_model_governance.html*; Federal Deposit Insurance Corporation, Supervisory Insights – Fair Lending Implications of Credit Scoring Systems (last updated Apr. 11, 2013), available at: *https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum05/article03_fair_lending.html*.

eligibility and credit decisions.[397] The prevalence of errors from such data is not currently known, though even traditional credit bureau information may have meaningful rates of errors.[398]

Recommendations

Treasury recognizes that these new credit models and data sources have the potential to meaningfully expand access to credit and the quality of financial services. Treasury therefore recommends that federal and state financial regulators further enable the testing of these newer credit models and data sources by both banks and nonbank financial companies.

Regulators, through interagency coordination wherever possible, should tailor regulation and guidance to enable the increased use of these models and data sources by reducing uncertainties. In particular, regulators should provide regulatory clarity for the use of new data and modeling approaches that are generally recognized as providing predictive value consistent with applicable law for use in credit decisions.

Regulators should in general be willing to recognize and value innovation in credit modelling approaches. Such approaches can create more robust risk management environments and improve both the cost and access to credit. Regulators should enable prudent experimentation with the aim of working through various issues raised, which may in turn require new approaches to supervision and oversight.

Given that consumers without credit scores tend to make regular monthly payments to telecom, utility, or rental companies and may benefit from the reporting of these fields, Treasury supports continued industry efforts to capture this type of additional consumer credit data through regular reporting to the consumer credit bureaus. Similarly, Treasury supports efforts to report monthly credit card payment amounts to the consumer credit bureaus to provide an additional level of granularity into consumer credit utilization.

Credit Bureaus

Overview

The consumer credit bureaus are essential to the functioning of consumer credit markets in the United States. Credit bureaus have not only become a vital resource for financial market participants such as lenders and servicers, but are also increasingly relied upon by property management companies and employers. Credit bureaus collect, store, and analyze consumer financial data including repayment history, outstanding debt, and other factors to produce a profile of a consumer's credit history. Today, about 189 million American consumers have credit reports with

397. Letter from Consumer Bankers Association, *Response of the Consumer Bankers Association to the Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process (Docket No. CFPB-2017-0005)* (May 19, 2017), at 9, available at: *https://www.regulations.gov/document?D=CFPB-2017-0005-0073*.

398. See, e.g., Bureau of Consumer Financial Protection, *Supervisory Highlights Consumer Reporting Special Edition* (Winter 2017), available at: *https://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf*.

sufficient information for the calculation of a credit score.[399] Credit bureaus also maintain files on another 19 million Americans who are considered "unscorable" due to insufficient information.[400] In total, nearly 210 million Americans rely on the three major consumer credit bureaus to accurately reflect their credit histories so that this history can be used by credit scorers and financial institutions to model credit risk, determine eligibility for credit, and establish the price of that credit. These entities collect significant amounts of personal and financial data about consumers, and, as a result, have a statutory requirement to protect consumer information in their possession.

Regulatory Treatment

Credit bureaus are subject to federal and state regulation for consumer protection purposes. At the federal level, credit bureaus are subject to the FCRA, which governs how credit bureaus collect information regarding consumers, use the information, and share the information with third parties.[401] In 2012, the Bureau, using its "larger participants" authority, began supervising the largest credit bureaus for compliance with federal consumer financial protection laws.[402] Prior to 2012, credit bureaus were not routinely supervised at the federal level.

Credit bureaus must safeguard personal financial information and are subject to statutory data security standards. The FTC has actively used its authority to enforce data security provisions under Section 5 of the FTC Act[403] and pursuant to the FTC's "Safeguards Rule,"[404] which the FTC implemented under authority granted to it by section 501(b) of the Gramm-Leach-Bliley Act (GLBA).[405] While GLBA granted FTC rulemaking and enforcement authority regarding the security and confidentiality of customer information, GLBA did not grant FTC authority to conduct supervision of credit bureaus for compliance with GLBA data security standards and privacy requirements. A similar limitation exists with respect to the Bureau. Dodd-Frank granted the Bureau supervisory authority with respect to certain requirements of GLBA, including provisions regarding consumer privacy,[406] but did not grant authority with respect to section 501 of GLBA,

---

399. Credit Invisibles Report.

400. Id.

401. The FTC website provides a summary of consumer rights under the FCRA, available at *https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf*.

402. In its final rule [12 C.F.R. part 1090], the Bureau defined the consumer reporting market to include companies that collect, analyze, maintain, or provide consumer report or other account information used in a decision by another person for offering of any consumer financial product or service. At the time, the Bureau's larger participants rulemaking for credit reporting covered nearly 30 companies accounting for 94% of annual receipts in the market. See Defining Larger Participants in Certain Consumer Financial Product and Service Markets (Feb. 8, 2012) [77 Fed. Reg. 9592 (Feb. 17, 2012)].

403. 15 U.S.C. § 45(a); see also Federal Trade Commission, *Enforcing Privacy Promises*, available at *https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises* (last accessed June 27, 2018) (listing press releases for FTC enforcement actions relating to privacy).

404. 16 C.F.R. Part 314; see also Standards for Safeguarding Customer Information (May 22, 2002) [67 Fed. Reg. 36484 (May 23, 2002)].

405. In addition to enforcement actions to stop practices that are harmful to consumers, the FTC engages with industry participants through reports and educational tools and also conducts policy and legislative work.

406. See Bureau of Consumer Financial Protection, *Privacy of Consumer Financial Information - Gramm-Leach-Bliley Act (GLBA) Examination Procedures* (Oct. 2016), at 1, available at: *https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102016_cfpb_GLBAExamManualUpdate.pdf*.

which requires regulators to establish standards for the protection of nonpublic personal information.[407] As a result, neither the FTC nor the Bureau supervises credit bureaus for compliance with these GLBA section 501 data security requirements.

Issues and Recommendations

Data Security – Supervision and Enforcement

In July 2017, Equifax noticed suspicious activity on the portal they provide consumers for dispute resolution and engaged a cybersecurity firm to investigate the suspicious activity.[408] The firm found that consumers' personal information was disclosed to unauthorized parties from May 13 to July 30, 2017.[409] In total, almost 150 million consumers' names, social security numbers, dates of birth, addresses, gender, phone numbers, driver's license numbers, and email addresses were breached.[410] Hundreds of thousands of consumers' credit or debit card information and documents provided to Equifax by 182,000 customers related to dispute resolutions were breached.[411] This incident has highlighted the need for greater supervision of the consumer credit bureaus, especially relating to the protection of nonpublic personal information.

The FTC has deep expertise on privacy and data security for nonbank financial companies. The FTC exercises enforcement authority under GLBA with respect to some types of nonbank financial companies, including credit bureaus.[412] However, as noted earlier, credit bureaus are not subject to routine supervision by either the FTC or the Bureau with respect to the requirements implemented under section 501 of the GLBA for the protection of nonpublic personal information. Given the sensitive nature of the information credit bureaus collect, the bureaus have a heightened duty to protect the information they collect.

Recommendations

The FTC should retain its rulemaking and enforcement authority for nonbank financial companies under the GLBA. Additionally, Treasury recommends that the relevant agencies use appropriate authorities to coordinate regulatory actions to protect consumer data held by credit reporting agencies and that Congress continue to assess whether further authority is needed in this area.

Credit Education and Counseling

In 1996, Congress passed the Credit Repair Organizations Act (CROA) to help protect consumers against unfair or deceptive advertising and business practices by credit repair organizations. In

---

407. Dodd-Frank § 1002(12)(J).

408. Equifax Inc., *Press Release – Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes* (Sept. 15, 2017), available at: *https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/*.

409. Id.

410. Equifax Inc., *Form 8-K Current Report* (May 4, 2018), available at: *https://otp.tools.investis.com/clients/us/equifax/SEC/sec-show.aspx?Type=html&FilingId=12735591&CIK=0000033185&Index=10000*.

411. Id.

412. In recent years, the Bureau has also undertaken enforcement actions in the area of data security, pursuant to its unfair, deceptive or abusive acts or practices (UDAAP) authority. At present, detailed guidance for compliance with UDAAP, akin to the FTC's Safeguards Rule, is not available.

CROA's passage, Congress found that credit repair companies were creating economic hardships for some consumers who had engaged their services and that consumers should be provided with information to help make an informed decision about the purchase of credit repair services. CROA defines a credit repair organization as "any person who uses any instrumentality of interstate commerce or the mails to sell, provide, or perform (or represent that such person can or will sell, provide, or perform) any service, in return for the payment of money or other valuable consideration, for the express or implied purpose of (i) improving any consumer's credit record, credit history, or credit rating; or (ii) providing advice or assistance to any consumer with regard to any activity or service described in clause (i)," with certain exceptions.[413] Under CROA, any entity deemed to be a credit repair organization is subject to requirements regarding how it may engage with a consumer and actions it must take before accepting payment for services. The FTC and private plaintiffs may bring actions for violations of CROA under a strict liability theory.

Credit repair organizations claim to help consumers improve their credit report and credit score, often by indicating they can assist in removing negative, unfair, or inaccurate credit information from consumer credit reports, with some companies falsely claiming that their years of expertise or relationship with the consumer credit bureaus will result in a more favorable outcome than if the consumer pursued removing inaccurate information on their own. Generally, these credit repair services are offered at a significant cost to the consumer. It is important to note that under existing law, consumers can receive a free credit report from each of the three national credit bureaus on an annual basis and can work directly with each of the credit bureaus to dispute any inaccurate information found in their credit report. Regardless of whether a consumer engages with the credit bureau or a credit repair company, accurate, negative credit information cannot be removed from the consumer's credit report.

Recently, credit bureaus, including the three largest bureaus, have expanded their offerings of credit and financial education services directly to consumers. These services generally do not involve specific action taken by the credit bureau to repair or change a credit report or score, but instead provide advice and education on how to address behavior or issues that influence consumers' credit profiles.

In *Stout v. Freescore, LLC*, the U.S. Court of Appeals for the Ninth Circuit held that Freescore, an online provider of credit scores, reports, and consumer credit information, was a "credit repair organization" under CROA.[414] The court reasoned that, in order to fall within the definition of "credit repair organization" under CROA, a person need not actually provide a service aimed at improving a consumer's credit record, history, or rating, as long as it represents that it can or will provide such a service. Consequently, since Freescore "affirmatively represents that its services can or will improve, or help to improve, a consumer's credit record, history, or rating," the court held that it fell within CROA's definition of a credit repair organization.[415] The decision in *Stout v. Freescore* troubled credit bureaus and credit scorers offering credit counseling services because those services aim to help consumers prospectively improve their credit scores, potentially exposing these firms to legal liability under CROA. The court's interpretation of CROA's scope creates a risk

413. 15 U.S.C. § 1679a.

414. *Stout v. Freescore, L.L.C.*, 743 F.3d 680, 681-85 (9th Cir. 2014).

415. Id. at 685-86.

that these companies, which have valuable insight to provide consumers, will limit their credit counseling offerings.

While the credit bureaus and credit scoring companies can and do offer limited consumer credit counseling services, CROA inhibits innovation by unduly restricting legitimate product offerings. For example, CROA requires a three-day waiting period from the time a consumer signs up for credit counseling services with a credit repair organization to the time the consumer receives the service, and prohibits credit repair organizations from collecting payment for the performance of any service until the entirety of that service is completed. Further, CROA includes strict liability and private right of action provisions that have discouraged legitimate entities like consumer credit bureaus and credit scorers from providing greater credit counseling offerings due to concerns about potential liability under CROA.

Innovation and modernization of credit education and counseling are important developments to ensure consumers become sophisticated and responsible borrowers. While the proper application of CROA provides valuable consumer protections, CROA's expansive definition of "credit repair organization" has unnecessarily restricted entities with significant expertise in consumer credit (such as credit bureaus and credit scorers) from offering consumer credit education and counseling products.

Recommendations

Treasury recommends that Congress amend CROA to exclude the national credit bureaus and national credit scorers (i.e., credit scoring companies utilized by financial institutions when making credit decisions) from the definition of "credit repair organization" in CROA.

InsurTech

As the broader financial services sector invests heavily in technology, digitally enabled advances across the insurance industry have come to be known as "InsurTech." InsurTech is a broad term used to describe new technologies with the potential to bring innovation to the insurance sector and these advances may impact regulatory practices for insurance markets.[416] Industry stakeholders — including existing or "traditional" insurers, startups, intermediaries, regulators, and consumers — are all exploring how technological advancements can be leveraged to increase efficiency, offer better-tailored products to consumers, increase consumer choice, and provide more effective and efficient regulation. Technological innovation reportedly has now overtaken insurance regulation as the issue about which property and casualty insurer senior executives are most concerned.[417]

416. Organization for Economic Co-operation Development, *Technology and Innovation in the Insurance Sector* (2017), available at: *https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf*. Treasury, through the Federal Insurance Office, highlighted a number of examples where InsurTech is changing the business of insurance in its 2017 Annual Report, available at: *https://www.treasury.gov/initiatives/fio/reports-and-notices/Documents/2017_FIO_Annual_Report.pdf*.

417. See, e.g., KPMG, *A New World of Opportunity: The Insurance Innovation Imperative* (Oct. 2015), at 7, available at: *https://assets.kpmg.com/content/dam/kpmg/pdf/2016/01/the-insurance-innovation-imperative.pdf*.

Recent InsurTech developments have affected a wide variety of operations, from back-office operations — including data collection techniques and pricing algorithms — to digital platforms, claims-handling processes, and product offerings. Technological tools now used by insurance stakeholders include the Internet of Things, telematics, big data, robo-advisors, machine learning/artificial intelligence (AI), and blockchain. Business models and product offerings have also evolved to include peer-to-peer (P2P), usage-based, and on-demand insurance.

InsurTech startup funding is substantial, with $2.3 billion invested in 2017 alone.[418] Traditional insurers have helped drive this growth by investing in InsurTech startups, and many have established business units devoted exclusively to strategic investment in InsurTech ventures, the exploration of their own InsurTech initiatives, and/or partnerships with InsurTech "hubs" that bring together entrepreneurs, investors, and industry experts.[419] Entrepreneurs and investors from outside of the insurance industry have also taken note of the potential to use InsurTech to make the insurance supply-chain more efficient. InsurTech thus continues to attract considerable interest for both its potential to complement existing processes and its potential to disrupt.

Stakeholders have also observed that the United States' regulatory environment could limit innovation in the U.S. insurance sector, which could inhibit economic growth. Factors that potentially could restrict insurance innovation include: (1) high regulatory barriers to entry; (2) little flexibility for regulators to accommodate new products or technologies; (3) inconsistent laws and regulations (or the possibility of inconsistent application of laws and regulations) across the 50 states; and (4) lengthy product approval processes. As a result, in some cases, insurers and startups prefer the regulatory practices of foreign jurisdictions, such as the United Kingdom or Singapore, over the United States when testing or introducing a new product or practice.

In response to InsurTech developments, insurance regulators are examining technological innovation and its potential regulatory impact. In the United States, state insurance regulators and the National Association of Insurance Commissioners (NAIC) have taken preliminary steps to better understand emerging technologies and their regulation.[420] The NAIC, for example, has formed an Innovation and Technology Task Force, which will, among other things, "[p]rovide a forum for the discussion of innovation and technology developments in the insurance sector, including the collection and use of data by insurers and state insurance regulators — as well as new products, services and distribution platforms — in order to educate

418. See, e.g., Deloitte, *Fintech by the Numbers: Incumbents, Startups, Investors Adapt to Maturing Ecosystem* (2017), available at: *https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-dcfs-fintech-by-the-numbers-web.pdf*; Willis Towers Watson, *Quarterly InsurTech Briefing Q4 2017* (Jan. 2018), available at: *https://www.willistowerswatson.com/-/media/WTW/PDF/Insights/2018/01/quarterly-insurtech-briefing-q4-2017.pdf*.

419. See, e.g., Oliver Suess, *InsurTech Startups Attract Growing List of Traditional Insurer Partners*, Ins. J. (Nov. 28, 2016), available at: *https://www.insurancejournal.com/news/international/2016/11/28/433226.htm*; Sam Boyer, Traditional Insurance City Set to Become Disrupting Insurance City, Insurance Business America (Dec. 13, 2017), available at: *https://www.insurancebusinessmag.com/us/news/technology/traditional-insurance-city-set-to-become-disrupting-insurance-city-87629.aspx*.

420. State regulation of the insurance industry is coordinated through the NAIC, a voluntary organization whose membership consists of the chief insurance regulatory officials of the 50 states, the District of Columbia, and the five U.S. territories.

state insurance regulators on how these developments impact consumer protection, privacy, insurer and producer oversight, marketplace dynamics and the state-based insurance regulatory framework."[421] The International Association of Insurance Supervisors (IAIS)[422] has also taken an interest in innovation and recently published a report titled "Fintech Developments in the Insurance Industry."[423]

Lawmakers, policymakers, and regulators should also take coordinated steps to encourage the development of innovative insurance products and practices in the United States. Domestically, this includes consideration of improving product speed to market, creating increased regulatory flexibility, and harmonizing inconsistent laws and regulations. Treasury's Federal Insurance Office, which provides insurance expertise in the federal government, should work closely with state insurance regulators, the NAIC, and federal agencies on InsurTech issues.

Payments

Overview of the U.S. Payments System

The United States is the leader in facilitating consumer and business payment transactions. In 2016, interbank payments systems in the United States handled over $1 quadrillion in transaction value, with payment systems involving nonbanks handling nearly $190 trillion of that transaction value.[424] Payments are essential to commerce and the payments infrastructure that has been built over decades empowers consumer choice in payments. This system has proven, over time, to be stable, secure, and effective.

In the United States, four primary core payment systems transfer value between financial institutions: credit card networks, debit card networks, automated clearing house (ACH) transfers, and wire transfer services. In addition to these core components, nonbank payment processors, payment service providers, money transmitters, and others help drive payment speed, security, efficiency and global penetration for businesses and consumers alike.

Recently, new technologies, especially in commerce, have changed the way that people live, consume, and pay for goods and services. New technological abilities have led to higher consumer expectations as to the speed and convenience of systems such as payments. Financial systems have

421. See *http://www.naic.org/cmte_ex_ittf.htm.*

422. Established in 1994, the IAIS is the international standard-setting body responsible for developing and assisting in the implementation of principles, standards, and other supporting material for the supervision of the insurance sector. The IAIS's objectives are as follows: to promote effective and globally consistent supervision of the insurance industry; to develop and maintain fair, safe, and stable insurance markets; and to contribute to global financial stability. IAIS members include insurance supervisors and regulators from more than 200 jurisdictions in approximately 140 countries.

423. International Association of Insurance Supervisors, *FinTech Developments in the Insurance Industry* (Feb. 21, 2017), available at: *https://www.iaisweb.org/file/65440/report-on-fintech-developments-in-the-insurance-industry*.

424. Bank for International Settlements Committee on Payments and Market Infrastructures, *Statistics on Payment, Clearing and Settlement Systems in the CPMI Countries* (Dec. 2017), at 406 and 408, available at: *https://www.bis.org/cpmi/publ/d172.pdf*.

and will continue to evolve to meet market demand, and payments is an area where innovation and disruption by nonbank and technology firms has been increasingly visible. Over the past few years, many firms have either launched a payments solution, or have publicly expressed interest in entering the payments ecosystem. Firms see a need and a demand for services that are faster, more convenient, and more integrated. As such, the breadth of available options coupled with the competition in payments has led to increased functionality, innovative solutions, and newer ways to ease transactions in order to promote economic activity and growth.

However, barriers to entry and innovation do exist in payments. First, a business case must be made before a firm even begins to build and implement a payment solution — scale of consumer adoption, ubiquity of acceptance, and security of the mechanism, among other challenges — must be taken into account for any new and innovative payment scheme to be successful.

Second, the payments system in the United States is operationally complex — while the payments landscape continues to undergo rapid innovation, there has been very little relative change to the back-end processes that actually move value throughout the financial system. Innovation in payments has largely been happening on the front-end, consumer-facing side of a transaction. The user experience, products, and innovative solutions that have been introduced in recent years with the advent of mobile technology, in essence, layer on top of the existing core payment systems.

Third, regulation of payments is fragmented; further, the core payment systems exist to move money between financial institutions and their customer accounts and as such, only regulated financial institutions have direct access to the infrastructure. To ensure the security of the payments system, those firms that directly connect to it must be safe and sound institutions that are adequately supervised; financial institutions as direct participants, therefore, are subject to prudential bank regulation and supervision. Firms that layer on top of this bank-centric system and provide consumer-facing solutions are regulated in a variety of ways, and governance of payments is as fragmented as the payment systems themselves. Payments firms are generally overseen through the banking agencies' third-party oversight guidance, through state money transmitter statutes, and/or by private payment network association operating rules and contracts. This fragmented approach to payments governance has perhaps in some ways entrenched legacy systems and slowed down innovations in areas like faster payments, but on the other hand, such a system has allowed for innovations over a wide range of niches that allow for multiple solutions to emerge and be tested by a wider audience. This can ensure innovation with fewer risks to payment safety.

Innovation has progressed through solutions built on top of the legacy payments infrastructure. There are benefits and challenges in employing such an approach; while the infrastructure, legal, and regulatory hurdles are very complex, this method has also allowed for more expediency than a built-from-scratch system and has allowed private firms to innovate on their own without extensive government mandates. See ***Appendix C*** for additional background on the U.S. payments systems.

Money Transmitters

Money transmitters are generally nonbank firms that transfer funds or value between individuals. These firms are important because they allow for payments to be made through a variety of channels and can be offered by various nonbank firms. In most cases, a nonbank that is moving

monetary value, whether it be by remittance (domestic or international), stored value/prepaid cards, check cashing, or person-to-person payments, will be licensed as a money transmitter.

Licensing and Supervision

Money transmitter licensing is governed primarily by state law. Differences in state statutes mean that there is no unified definition of a money transmitter; as a result, states have different variations that could bring in a number of firms that do not necessarily engage in the traditional form of funds transfer. If a firm engages in money transmission, or even if it may potentially fall under the definition of a money transmitter in a certain state, then it must apply for a money transmitter license in that state, in many cases without even having a physical presence in the state. The effect is that for any firm with a nationwide footprint, a license in every state is necessary. Licensing requirements vary by state, but generally include requirements to submit credit reports, business plans, and financial statements; and a requirement to maintain a surety bond to cover losses that might occur. States have engaged in several efforts to streamline the licensing process, but overall adoption of these initiatives has been mixed. (Further discussion of state licensing of money transmitters is addressed in the previous chapter on Aligning the Regulatory Framework to Promote Innovation.)

Money transmitters are considered money services businesses (MSBs) and are therefore subject to the requirements of the Bank Secrecy Act. They must register at the federal level with FinCEN. Banks, foreign banks, or firms that are registered with the U.S. Securities and Exchange Commission (SEC) or U.S. Commodity Futures Trading Commission (CFTC) are not considered MSBs and do not have to register as such.

Money transmitters are supervised and examined by each state where they hold a license. For money transmitters with nationwide state licenses, this means duplicative examinations by a number of different state regulators, and has emerged as a common theme for reform among firms. The most recent data available from state regulators shows that over half of all consolidated money transmitter firms operate and have licenses in multiple states.[425]

State regulators note that while states have different frequency of exams, most money transmitters are examined annually, either by individual states and/or through joint exams organized among several states. States examine for safety and soundness as well as compliance with both state law and BSA/AML requirements.[426] Firms have raised concerns regarding the frequency and quantity of examinations and the sometimes-differing standards and idiosyncratic requirements from state to state.

Regulation E Remittance Rule Disclosures

For money transmitters that provide international remittances, a particular regulatory inefficiency has emerged after financial reform. Section 1073 of Dodd-Frank requires disclosures to be provided

425. Conference of State Bank Supervisors and Money Transmitters Regulators Association, *The State of State Money Service Businesses Regulation and Supervision* (May 2010), at 6, available at: *https://www.csbs.org/state-state-money-service-businesses-regulation-and-supervision*.

426. Id. at 9-10.

to senders of remittance transfers.[427] The Bureau implemented section 1073 through amendments to Regulation E to require that:

- Companies give disclosures to consumers before the consumers pay for the transfer. These disclosures must include: the exchange rate, fees and taxes collected, fees charged by agents and intermediaries, the amount of money delivered not including fees and taxes charged to the recipient, and a disclaimer that other fees may apply.
- Companies also provide a post-transaction receipt that repeats all the information from the first disclosure, plus dates of payment availability, and error resolution and cancellation rights notices.
- Companies generally give customers 30 minutes to cancel a transfer in exchange for a full refund.[428]

The rule applies to any electronic transfer of funds from a U.S.-based customer to a person in a foreign country; this includes both money transmitters and banking organizations and applies even if done through a wire transfer or ACH. There is, however, a de minimis exemption for transfers of $15 or less and companies that performed 100 or fewer remittance transfers in the current and previous calendar year.[429] Firms have noted concerns with the lack of flexibility in the disclosure rules. For example, electronic disclosures, like an email or mobile disclosure, may only be given if the transaction is done electronically. For in-person transactions, paper receipts must be provided.

Recommendations

Treasury supports the Bureau's ongoing efforts to reassess Regulation E. Treasury recommends that the Bureau provide more flexibility regarding the issuance of Regulation E disclosures and raise the current 100 transfer per annum threshold for applicability of the de minimis exemption.

Fintech and Payments

Technology has advanced the payments market, increased competition, and increased innovation as new payment services have been introduced and further layered upon the existing payments system. Many new firms and technologies are now competing for a greater share of consumer transactions and the corresponding data. Thus far, few dominant players have yet emerged, and fintech payments solutions have largely remained confined to niche uses within the market.

Person-to-Person (P2P) Payments

P2P payments that move money directly between bank accounts have been relatively slow to develop in the United States, in large part due to challenges within the existing payments infrastructure. Two core payment systems used to transfer funds between bank accounts — wire transfers and ACH — each have challenges for P2P. For example, wire transfers are far more expensive than ACH. On the other hand, ACH does not transfer in real time like wire transfers. Both methods require that the receiver provide the sender with their bank account information — routing and account numbers

427. 12 U.S.C. § 5601.

428. 12 C.F.R. §§ 1005.30-1005.36.

429. Id. § 1005.30.

— which may be cumbersome to find and may raise security concerns. More recently, technology and innovation have provided a way for a competitive market for P2P payments to emerge.

Like many other innovations in the payments system, these new P2P technologies layer on top of the existing payment systems. These new products are filling a demand for better account-to-account transfer mechanisms and consumer experience, and are beginning to build scale. According to a consumer payments survey, P2P payments are gaining ground, but mostly among young consumers. The survey found that the breakdown of P2P payment adopters fell largely along lines of age demographics, as people under the age of 35 were far more likely to already use or be ready to adopt P2P payment platforms than consumers over the age of 55.[430] However, there is room for growth, as only 29% of those surveyed have completed a P2P payment, with slightly less than half of the under-35 demographic having already used such a service. Among respondents who had not used a P2P payment service in 2017, more than half of those between 18 and 55 said that they were likely or somewhat likely to use such a service in the future. Security concerns are more likely to hold back older users from using P2P payments than other types of concerns.[431]

Innovative solutions to these problems have begun to emerge in the market and additional innovation in this space is to be expected. While multiple options exist in the market, two well-known examples are discussed.

Bank Account-to-Bank Account Transfers

A consortium of some of the largest U.S. banks[432] has been working on a mechanism to transfer funds quickly and directly between bank accounts. The system works by leveraging the debit card infrastructure to move money, and generally functions through the online and mobile banking portals of each member bank. Previously, account-to-account transfers have needed to use either the wire transfer or ACH networks to complete the transaction. But now, the new transactions are cleared and posted in near real time and settlement occurs bilaterally between the applicable banks at the end of the day via ACH; in essence, the new network serves as a special standardized messaging system between banks for specific account-to-account transfers.

Nonbank P2P Transfers

A number of MSBs have also emerged in the P2P space. These nonbank firms usually have obtained money transmitter licenses in every state, and only allow users to transfer money to other users of the same service. These sorts of services work by first using the balance that is held in a user's account; if the account does not have enough funds, an ACH transfer from a bank account or funding with a debit card or a credit card, can be used as a funding option.[433]

---

430. Total System Services, Inc., *2017 TSYS U.S. Consumer Payment Study* (Mar. 27, 2017), at 13-14, available at: *https://www.tsys.com/Assets/TSYS/downloads/rs_2017-us-consumer-payment-study.pdf* ("TSYS Payment Study").

431. Id.

432. Bank of America, BB&T, Capital One, JPMorgan Chase, PNC Bank, U.S. Bank, and Wells Fargo Bank. See Early Warning Services, LLC, *Early Warning Corporate Overview* (2017), available at: *https://www.earlywarning.com/pdf/early-warning-corporate-overview.pdf*.

433. See, e.g., PayPal, Inc., *Venmo User Agreement* (last updated Dec. 18, 2017), available at: *https://venmo.com/legal/us-user-agreement*.

Digital Wallets

Digital and mobile wallets have increased in popularity and have continued to evolve within the last few years. Researchers at the Federal Reserve Bank of Boston have categorized mobile wallets into four distinct models: (1) near field communication (NFC) wallets; (2) cloud-based, card-on-file wallets; (3) cloud-based, card-on-file card network wallets; and (4) merchant or financial institution QR code-based wallets.[434] Each of these methods uses tokenization to secure payment information.

- NFC wallets are contactless payment mechanisms. Payments are made when a smartphone is held near a payment terminal, and authentication takes place (fingerprint or PIN number) before the information is sent from the phone to the terminal. NFC wallets have a number of common features, although the hardware and software vary. NFC wallets can only accept eligible and wallet-accepted credit and debit cards, are available for use where a retailer has an NFC-enabled payment terminal, and can only be used with the corresponding smartphone operating system.[435]
- Cloud-based, card-on-file wallets are primarily used for online e-commerce payments. These services allow a consumer to utilize multiple funding methods — credit/debit/prepaid cards, ACH, and so on — for input into the mobile wallet. The consumer may then check out at various merchants online using the funding method of their choice within the wallet. Generally, any payment card may be input – there is not a need for the issuing bank to provide for eligibility. Merchants utilize APIs to enable payment using these services.[436]
- Cloud based, card-on-file card network wallets function similar to the card-on-file systems previously noted, removing the need for merchants to store and collect payment data. The card networks work with merchants to allow for the digital wallets to be enabled on their own website or mobile app.[437]
- QR code-based wallets use QR codes as a way to complete payment, with payment information that is stored in the app. These services, however, can only be used in their own environments. For bank-based wallets, a QR code provided by the app must be scanned by the cashier, and can only be used in conjunction with the financial institution's products. A store-based payment app requires the consumer to scan the QR code provided by the store's payment terminal to complete the payment.[438]

Like P2P payments, digital wallets are also seeing increased adoption among younger consumers, albeit very gradually. Age is a significant factor in the likelihood that a particular consumer has loaded or plans to load card information into a digital wallet. As for funding choice, consumers are

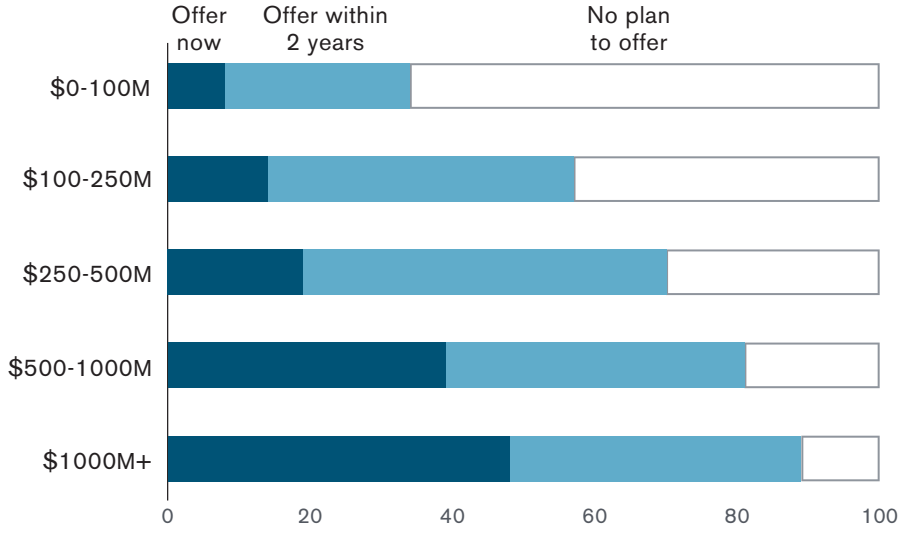
---

434. Susan M. Pandy and Marianne Crowe, Federal Reserve Bank of Boston, *Adapting to Mobile Wallets: The Consumer Experience* (revised June 16, 2017), available at: *https://www.bostonfed.org/publications/payment-strategies/choosing-a-mobile-wallet-the-consumer-perspective.aspx*.
435. Id. at 5.
436. Id. at 13.
437. Id. at 16.
438. Id. at 18-20.

more likely to load a credit card into a digital wallet than a debit card, and far more likely to use a credit card to make an online payment.[439]

For mobile wallet usage (especially NFC wallets) to increase, the cards that are issued by banks must be eligible for enrollment. In 2017, the Federal Reserve Bank of Boston released a survey that asked banks from across the United States about their plans for mobile payments, among other things. The survey found that a relatively small percentage of banks offered mobile wallet services, and those that did were predominantly larger banks.

Figure 23: U.S. Financial Institutions Mobile Payment Services Plan (percent of respondents by asset size)

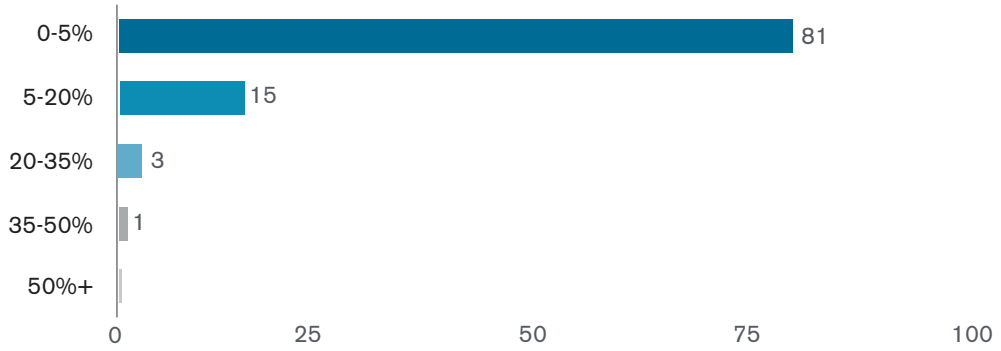


Source: Marianne Crowe et al., *Mobile Banking and Payment Practices of U.S. Financial Institutions 2016 Mobile Financial Services Survey Results from FIs in Seven Federal Reserve Districts,* Federal Reserve Bank of Boston (Dec. 2017), at 50.

439. TSYS Payment Study, at 13-14.

Also, as shown in **Figure 24** below, the survey found that at banks that offer mobile payment services and track customer usage data, a small percentage of customers (vertical axis) account for a large proportion of mobile wallet usage (horizontal axis).[440]

Figure 24: Customer Enrollment in Mobile Payment Services (percent of respondents that track data)



Source: Marianne Crowe et al., *Mobile Banking and Payment Practices of U.S. Financial Institutions 2016 Mobile Financial Services Survey Results from FIs in Seven Federal Reserve Districts*, Federal Reserve Bank of Boston (Dec. 2017), at 60.

Despite the fragmented regulatory framework and layered nature of the overall system, payments have been an area of high innovation and competition, which thus far has been beneficial to consumers and the market. This competition has led to a number of private actors emerging that are capable of providing innovative services in new and different ways. Given the structure of the payments system in general, a wait-and-see approach to innovative payments may be most beneficial. The next steps in payments will likely center around the pursuit of more speed and security in payments.

Payments Modernization

Technology continues to evolve and transform the way that consumers in the United States and abroad do business. The increase in technological capacity and delivery systems has sped up the nature of even routine transactions. Today, one can shop, compare, transact, and receive delivery faster than ever before — and the underlying technology will continue to advance in order to make this process even quicker and more efficient. However, as noncash transactions have increased, the back-end payments system underlying these transactions remains largely the same. As innovation allows for faster transactions, consumers are going to demand payments systems that likewise function with more speed.

440. Marianne Crowe, Elisa Tavilla, and Breffni McGuire, *Mobile Banking and Payment Practices of U.S. Financial Institutions: 2016 Mobile Financial Services Survey Results from FIs in Seven Federal Reserve Districts* (Dec. 2017), at 60, available at: *https://www.bostonfed.org/publications/mobile-banking-and-payment-surveys/mobile-banking-and-payment-practices-of-us-financial-institutions.aspx*.

Recognizing this, the Federal Reserve set out to lead a discussion on how best to modernize the U.S. payments system. The process started with the Federal Reserve releasing a consultation paper[441] for public comment in 2013. Following the comment period, the Federal Reserve issued a strategy document[442] that outlined desired outcomes and next steps for improving the payments system. In order to advance solutions for the five desired outcomes of speed, security, efficiency, ease of international payments, and collaboration, the Federal Reserve set up two task forces: one for faster payments and one for secure payments. While the Federal Reserve served as the leader and convener of these task forces, they were inclusive of a wide variety of stakeholders and perspectives so that they would result in collective agreement on a path forward.

Faster Payments Task Force

The Faster Payments Task Force was initially convened in May 2015 with the charge of identifying and evaluating approaches for implementing safe and ubiquitous faster payments capabilities. The task force consisted of over 300 stakeholders, and was initially given a deadline of 2016 for completing this work. Their final report was released in two parts in 2017: part one[443] discussed the task force's approach, and part two[444] outlined the task force's recommendations. The task force asked industry participants to submit proposals for faster payments solutions that firms had under consideration. The goal was not to select proposals as winners, but merely to identify ideas for solutions that private-sector participants were envisioning.

Industry Efforts on Faster Payments

The Clearing House's Real-Time Payments (RTP) System

In November 2017, The Clearing House's (TCH) RTP system — one of the private-sector, faster payments solutions proposed to the task force — went live as an entirely new payment system. Though RTP is open to all U.S. depository institutions, it currently connects six U.S. banks, and TCH has partnered with servicing firm FIS in order to expand the reach of RTP past TCH's membership base. RTP allows participants to send credit (push) payments through the system at any time with clearance, settlement, and availability/posting to the receiver in real time. RTP does not include a consumer-facing payment application; it is the back-end plumbing that moves payments between banks resulting from the banks' own customer-facing applications and services. One of the key components of RTP is the secure messaging system that allows banks to communicate with

441. Federal Reserve Banks, *Payment System Improvement – Public Consultation Paper* (Sept. 10, 2013), available at: *https://fedpaymentsimprovement.org/wp-content/uploads/2013/09/Payment_System_Improvement-Public_Consultation_Paper.pdf*.

442. Federal Reserve System, *Strategies for Improving the U.S. Payment System* (Jan. 26, 2015), available at: *https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf*.

443. Faster Payments Task Force, *The U.S. Path to Faster Payments Final Report Part One: The Faster Payments Task Force Approach* (Jan. 2017), available at: *https://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-final-report-part1.pdf*.

444. Faster Payments Task Force, *The U.S. Path to Faster Payments Final Report Part Two: A Call to Action* (July 2017), available at: *https://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-task-force-final-report-part-two.pdf*.

payment messages. The messages are flexible, compliant with global messaging standards,[445] and allow for immediate confirmation.

TCH is the rule writer for the RTP system.[446] System participants must be depository institutions with branches or offices located in the United States. While nonbank firms cannot be direct participants in RTP, TCH does have a process for allowing third-party processors to be used for transmitting and receiving messages through the system on behalf of their banking clients. Currently, payment values through the system are capped at $25,000 per transaction.

Banks are required to prefund a Federal Reserve account and participants must have Federal Reserve clearing accounts to use RTP (or have a relationship with a correspondent bank that can act as a funding agent). TCH uses a single pooled account at the Federal Reserve which is jointly owned by all participating banks (and/or funding agents), with TCH acting as the sole custodian. While all the banks have an ownership stake in the account, only TCH can approve or push money out to a bank. The account is pre-funded by the banks via Fedwire payment. The size of each bank's prefunding obligation is determined by TCH rules, and while it is envisioned that most banks will prefund once per day, provisions allow for multiple rounds of prefunding or top-up funding throughout the day.

Same Day ACH[447]

Over the past several years, the rule-writing organization for all ACH networks, NACHA, and the ACH operators have been working to bring more speed to ACH payments by introducing a same-day ACH service. In 2017, its first full year of availability, same-day ACH payments amounted to 75.1 million separate transactions with an aggregate value of $87.1 billion.[448]

Same-day ACH was implemented in three phases. The first phase (September 2016)[449] set up two new daily payment submission windows: a morning submission deadline at 10:30 a.m. ET, with settlement occurring at 1 p.m.; and an afternoon submission deadline at 2:45 p.m. ET, with settlement occurring at 5 p.m. The first phase was limited to credit (push) transactions, and mandated that every receiving financial institution be able to accept same-day ACH transfers and make the funds available to customers at the end of its processing day. The second phase (September 2017)[450]

---

445. Specifically, the messages are compliant with ISO 20022, which is a universal financial industry messaging scheme that enables financial systems around the world to communicate through a common messaging protocol.

446. The Clearing House, *Real-Time Payments Operating Rules* (Oct. 30, 2017), available at: *https://www.theclearinghouse.org/payment-systems/-/media/6de51d50713841539e7b38b91fe262d1.ashx*; The Clearing House, *Real-Time Payments Participation Rules* (Oct. 30, 2017), available at: *https://www.theclearinghouse.org/payment-systems/-/media/d0314d2612ab4619b3c09745b54cf96f.ashx*.

447. See ***Appendix C*** for more background on the ACH system.

448. NACHA, *Same Day ACH Volume 2017* (Jan. 11, 2018), available at: *https://web.nacha.org/resource/same-day-ach/same-day-ach-volume-2017*.

449. NACHA, *Same Day ACH: Moving Payments Faster (Phase 1)* (Sept. 23, 2016), available at: *https://www.nacha.org/rules/same-day-ach-moving-payments-faster*.

450. NACHA, *Same Day ACH: Moving Payments Faster (Phase 2)* (Sept. 15, 2017), available at: *https://www.nacha.org/rules/same-day-ach-moving-payments-faster-phase-2*.

allowed debit (pull) entries to be originated. The third and final phase (March 2018)[451] mandated that all same-day ACH funds be made available to customers by 5 p.m. local time for each receiving financial institution. Currently, international transactions and single transfers exceeding $25,000 are not eligible for same-day ACH.

Although the same-day ACH project has been completed, NACHA continues its focus on increasing the speed of payments. In early 2018, NACHA asked for member comment on a proposed new rule that would: (1) add a third same-day ACH submission window with a deadline at 5:15 p.m. ET and settlement occurring at 6:30 p.m.; (2) mandate 1 p.m. local time funds availability for the first ACH settlement window; and (3) increase the eligible transaction cap to $100,000.

Challenges for Faster Payments in the United States

Adoption and Acceptance

In any payment system, one of the key challenges is the level of consumer adoption of the system. If a payment system does not have broad adoption by consumers, then merchants have less incentive to expend resources to accept it. Likewise, consumers are less likely to use a payment method if it is not widely accepted. One factor that can mitigate this problem is if there is interoperability between systems, and providers can at least receive payments on behalf of customers. Without a mandate, either from the government or a large share of private sector operators, change can be much slower. For example, same-day ACH had a very low adoption level until NACHA amended its rules to require receipt.[452] Similarly, it was the private credit card networks that initiated the liability shift for EMV cards over the last few years. U.S. government entities have opted not to create mandates, instead preferring a collective approach.[453]

Use Cases

Another challenge to faster payments is the lack of clear business and use cases for faster payments, aside from emergency payments. As a part of its payments improvement work, the Federal Reserve commissioned consultants to study the question of use cases. First, the consultants noted that among countries that have established faster payments, the decision was more strategic than based on use cases and that premium pricing was likely to affect adoption, among other factors.[454] When discussing business cases, the consultants found that they were net neutral or even net negative given the conservative assumptions used, but that business cases could be net positive if the time horizon were expanded.[455] They did note however, that latent demand could be a challenge in the analysis — that demand could emerge in the market after the new

---

451. NACHA, *Same Day ACH: Moving Payments Faster (Phase 3)* (Mar. 16, 2018), available at: *https://www.nacha.org/rules/same-day-ach-moving-payments-faster-phase-3*.

452. Faster Payments Task Force Final Report Part Two, at 17-18.

453. Federal Reserve System, *Strategies for Improving the U.S. Payment System: Federal Reserve Next Steps in the Payments Improvement Journey* (Sept. 6, 2017), available at: *https://fedpaymentsimprovement.org/wp-content/uploads/next-step-payments-journey.pdf*.

454. Federal Reserve System, *Strategies for Improving the U.S. Payment System* (Jan. 26, 2015), at 37-38, available at: *https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf* ("Federal Reserve 2015 Strategies").

455. Id. at 43-44.

technology and infrastructure is introduced, similar to the U.K.'s experience where payments technology allowed for a shift to a "just-in-time" product delivery model that lessened the need for excess small business working capital.[456]

Cost

Today, faster payments services are more expensive to use. Taking the ACH system as an example, next-day batched ACH through the Federal Reserve's FedACH system costs $0.0035 per transaction (although there is tiered pricing, and discounts are available for higher volumes),[457] whereas the same-day ACH service costs $0.052 per transaction.[458] This difference in cost is why the majority of ACH payments made by Treasury, for example, through FedACH may not be suitable for same-day servicing.

Settlement

Post-transaction settlement refers to the payment of obligations between parties. This can be done in one of two ways — between private banks or through a country's central bank, with the latter seen as less risky. When it comes to faster payments, the United States, unlike some other jurisdictions, does not currently have a 24x7x365 real-time settlement system. Real-time settlement can reduce credit risk that institutions otherwise have to take once payments are cleared and posted to the receiver's account in real time.

The Federal Reserve Banks own and operate the National Settlement Service (NSS), which provides multilateral settlement for private-sector clearing arrangements, including private ACH networks. Unlike Fedwire, which settles immediately upon payment under a Real-Time Gross Settlement framework, the NSS is a deferred net settlement system, which means that payments are accumulated and netted throughout the day (or period if more frequently than daily), until net settlement occurs.[459] The NSS is open for use Monday-Friday from 7:30 a.m.-5:30 p.m., ET.[460]

In the Federal Reserve's payments strategy document, they note that the NSS expanded its daily opening times by a half hour at open and close during 2015, and that the Fed would look into weekend and 24x7x365 service in the future.[461] To date, available hours have not been expanded further.

The European Central Bank is developing an instant payments settlement system that is scheduled to go live in November 2018. The TARGET Instant Payment Settlement service will be available 24x7x365.[462]

---

456. Id. at 44-45.

457. FedACH, *Services 2018 Fee Schedule*, accessible at: *https://www.frbservices.org/resources/fees/ach-2018.html*.

458. NACHA, 2016, *Same Day ACH: FAQ*, at 3, accessible at: *https://web.nacha.org/system/files/resource/2017-08/Same-Day-ACH-FAQ-2016_0.pdf*.

459. Bank for International Settlements Committee on Payment and Settlement Systems, *Principles for Financial Market Infrastructures* (Apr. 2012), at 149-150, accessible at: *https://www.bis.org/cpmi/publ/d101a.pdf.*

460. Board of Governors of the Federal Reserve System, *National Settlement Service* (last updated Jan. 15, 2015), available at: *https://www.federalreserve.gov/paymentsystems/natl_about.htm*.

461. Federal Reserve 2015 Strategies, at 50-52.

462. European Central Bank, *The New TARGET Instant Payment Settlement (TIPS) Service* (June 2017), available at: *https://www.ecb.europa.eu/paym/intro/news/articles_2017/html/201706_article_tips.en.html*.

Recommendations

Treasury agrees with the approach taken by the Faster Payments Task Force and notes that collective action and agreement can be a very powerful tool in creating a faster payments system that works for all stakeholders. However, now that the foundational work has been completed, Treasury recommends that the Federal Reserve set public goals and corresponding deadlines consistent with the overall conclusions of the Faster Payments Task Force's final report.

Treasury recommends that the Federal Reserve move quickly to facilitate a faster retail payments system, such as through the development of a real-time settlement service, that would also allow for more efficient and ubiquitous access to innovative payment capabilities. In particular, smaller financial institutions, like community banks and credit unions, should also have the ability to access the most-innovative technologies and payment services.

While Treasury believes that a payment system led by the private sector has the potential to be at the forefront of innovation and allow for the most advanced payments system in the world, back-end Federal Reserve payment services must also be appropriately enhanced to enable innovations. Treasury agrees with the Federal Reserve's policy criteria for introducing a new payment service – namely, that the Federal Reserve must: (1) expect to achieve full cost recovery in the long run; (2) expect the service to provide a clear public benefit, including improving the effectiveness of markets, reducing the risk in payments, or improving efficiency of the payments system; and (3) conclude that the service should be one that other providers alone cannot expect to provide with reasonable effectiveness, scope, and equity.[463]

Faster Payments Abroad

Many jurisdictions around the world have embarked on initiatives to increase the speed of payments. In many cases, the progress towards faster payments abroad has outpaced progress in the United States. As of mid-year 2017, it is estimated that there were 25 countries that had some sort of live faster payments system. Features of these faster payment systems vary, but most systems are operational 24/7 and post transactions to accounts in real time, near real time, or within a few minutes.[464] At the same time, it is estimated that there were 10 additional countries that had faster payments systems under development, including the United States.[465]

The United Kingdom's Transition to Faster Payments

One such system, the U.K. Faster Payments Scheme, is worth looking at in more detail as its transition could provide an interesting comparison to the current U.S. payments system. The U.K. Faster Payments Service (FPS) was created as an entirely new infrastructure on a directive

463. Board of Governors of the Federal Reserve System, *Federal Reserve in the Payments System*, Policy Statement (1990), available at: *https://www.federalreserve.gov/paymentsystems/pfs_frpaysys.htm*.

464. FIS, *Flavors of Fast: A Trip Around the World of Immediate Payments* (2017), at 29-55.

465. Id. at 66-71. This estimate was made prior to TCH's RTP system going live, although RTP is still currently limited to a small number of member banks.

from the government, and went live in 2008.[466] Prior to the implementation of FPS, the U.K. had a payment rail network that was very similar to the current U.S. system. The U.K. large value Real-Time Gross Settlement system, CHAPS, is very similar to Fedwire and CHIPS. The U.K. batched electronic payment transfer network, Bacs, is very similar to the U.S. ACH networks.[467]

The process to build and implement FPS took about three years, from directive to an operational system.[468] The United Kingdom first considered options to speed up account to account payments through systems that were already operational. While they considered speeding up Bacs to same-day service, or promoting more usage of CHAPS for lower value payments, problems of ultimate speed and cost to the consumer, respectively, pushed them to choose the path of creating a brand new infrastructure.[469] The FPS system authorizes and clears transactions in real time, but settlement is still deferred and done through the Bank of England's three daily settlement cycles, as was done prior to FPS. The most recent annual data from FPS shows that the service is growing the fastest of any form of electronic payment in the United Kingdom, having logged 16% growth between 2016 and 2017.[470]

One notable difference between the U.K. FPS and a potential U.S. faster payments system is the ability for widespread adoption. Since the U.K. banking system is more concentrated than the U.S. banking system, a U.S. system would need to be reachable by a larger number of banking institutions to benefit all consumers, and the cost to operate the system would have to be borne by a greater number of institutions which could lead to higher costs of implementation and maintenance.[471] While the United Kingdom provides an example for implementation of a faster payments network, many of these issues may have different outcomes in a U.S. system.

Cross Border Faster Payments

Most payments systems work within the borders of a single country and transfer units of a single currency. However, there are systems that are in development and beginning to come online that will allow for faster transfer of funds across borders and currencies. One example is the SWIFT GPI enhanced messaging system, which went live in January 2017. SWIFT currently has over 150 banks worldwide that are committed to the service, and 45 banks that are live. The SWIFT GPI systems allows for faster crediting of funds (50% credited within 30 minutes), unaltered remittance information, complete directories of members, and tracking of payments through the entire process.[472]

---

466. Claire Greene et al., *Costs and Benefits of Building Faster Payments Systems: The U.K. Experience and Implications for the United States*, Federal Reserve Bank of Boston Current Policy Perspectives No. 14-5 (Feb. 24, 2015), at 2, available at: *https://www.bostonfed.org/publications/current-policy-perspectives/2014/costs-and-benefits-of-building-faster-payment-systems-the-uk-experience-and-implications-for-the-united-states.aspx*.
467. Id. at 10-11.
468. Id. at 28.
469. Id. at 30-31.
470. For additional statistics for FPS growth and volumes, see *http://www.fasterpayments.org.uk/statistics*.
471. Greene et al., at 44-46.
472. See SWIFT, *SWIFT gpi: Cross-Border Payments, Transformed* (Mar. 2018), available at: *https://www.swift.com/resource/swift-gpi-brochure*.

Secure Payments Task Force

The Secure Payments Task Force was initially convened in June 2016 and focused on three priorities: (1) identifying payment security priorities; (2) advising the Federal Reserve on payment security; and (3) coordinating with the Faster Payments Task Force.[473] The group included stakeholders from both government and the private sector. The Federal Reserve acted as a facilitator and convener. The Secure Payments Task Force issued its final deliverable in March 2018 — an educational report on the payment lifecycle and security profiles of various payment methods including legal and regulatory references for each category of payment, and a short, high-level list of challenges and improvement opportunity within each payment bucket.[474] After issuing the report, the task force disbanded.

In March 2018, the Federal Reserve announced a 4-6 month study to measure and assess payments fraud and its costs, which is expected to provide insights into the vulnerability points within payment security.[475] The Federal Reserve also plans to establish collaborative industry workgroups on topics yet to be discussed. Other efforts to enhance payment security, such as EMV migration, have been accomplished through private sector channels.

Recommendations

Treasury recognizes the utility of a working group that is focused on the continued high level of security in the U.S. payments system. To this end, Treasury looks forward to specific next steps and actionable deadlines for continued work from members of the Secure Payments Task Force and similar groups. The Federal Reserve should work as the convener, coordinator, and driver of the work product produced by members that worked on the Secure Payments Task Force, which could include work streams identified by the Faster Payments Task Force as areas for future work. Specifically, the Federal Reserve should engage stakeholders to identify payment systems resiliency as new payment systems come online, and to help counsel the Federal Reserve as it works to potentially develop its own operating faster payments system. The Federal Reserve should continue to engage stakeholders to promote and develop mechanisms to improve information sharing within the payments ecosystem, and especially between members of the improved payments task forces. Treasury recommends that continued work in the area of payment security include an actionable plan for future work, and ensure that solutions, especially in security, do not include specific tech mandates.

---

473. Federal Reserve System, *Strategies for Improving the U.S. Payment System: Federal Reserve Next Steps in the Payments Improvement Journey* (Sept. 6, 2017), at 7, available at: *https://www.federalreserve.gov/newsevents/pressreleases/files/other20170906a1.pdf*.

474. Secure Payments Task Force, *Payment Lifecycles and Security Profiles* (Mar. 2018), available at: *https://securepaymentstaskforce.org/wp-content/uploads/sptf-profiles-all.pdf*.

475. Board of Governors of the Federal Reserve System, *Press Release - Federal Reserve to Study Payments Fraud and Security Vulnerabilities* (Mar. 29, 2018), available at: *https://www.federalreserve.gov/newsevents/pressreleases/other20180329a.htm*.

Wealth Management and Digital Financial Planning

Overview

One of the Core Principles outlined in Executive Order 13772 is to "empower Americans to make independent financial decisions and informed choices in the marketplace, save for retirement, and build individual wealth." Despite efforts at improving financial literacy, including through the Financial Literacy and Education Commission chaired by the Secretary of the Treasury,[476] many Americans struggle with making financial decisions that have a profound effect on their own well-being and the well-being of their dependents. Too often, individuals make financial decisions that are sub-optimal or based on immediate gratification rather than their long-term financial welfare.[477]

For decades, wealthier Americans have hired advisors to develop, implement, and monitor financial plans. Financial planning can involve a broad range of services, including recommendations for budgeting and goal setting, spending oversight, debt management, asset allocation for investment portfolios, selection of insurance products, and tax and estate planning; however, there is no universal definition as to what should be included in a financial plan.[478] There are also no legal requirements regarding the qualifications to be a financial planner. Some financial advisors may describe themselves as financial planners, but only recommend investments in a narrow range of products.[479]

In the past, the costs of retaining a financial planner may not have made economic sense for Americans with modest means. This lack of financial planning advice can often make it more difficult for these Americans to achieve sufficient wealth accumulation to sustain their livelihoods in retirement. To the extent that Americans do not adequately plan and save for their financial needs, additional stresses can be placed on the taxpayer-supported safety net. Disparities in access to financial expertise can lead to increased wealth inequality in the United States.

Trends in Retirement Savings

The benefits provided by Social Security were never intended to be the sole source for retirement income needs.[480] While Americans are responsible for covering the remainder of their retirement needs, a significant number are inadequately prepared.[481]

---

476. See generally *https://www.treasury.gov/resource-center/financial-education/Pages/commission-index.aspx*.

477. See Justine S. Hastings and Olivia S. Mitchell, *How Financial Literacy and Impatience Shape Retirement Wealth and Investment Behaviors*, NBER Working Paper (Jan. 2011), available at: *http://www.nber.org/papers/w16740.pdf*.

478. See U.S. Government Accountability Office, *Consumer Finance: Regulatory Coverage Generally Exists for Financial Planners, but Consumer Protection Issues Remain* (Jan. 2011), at 1, available at: *https://www.gao.gov/new.items/d11235.pdf*.

479. Office of Investor Education and Advocacy, U.S. Securities and Exchange Commission, *Investment Advisers: What You Need to Know Before Choosing One* (Aug. 7, 2012), available at: *https://www.sec.gov/reportspubs/investor-publications/investorpubsinvadvisershtm.html*.

480. Social Security Administration, *Understanding the Benefits* (2018), at 1, available at: *https://www.ssa.gov/pubs/EN-05-10024.pdf*.

481. YiLi Chien and Paul Morris, Federal Reserve Bank of St. Louis, *Many Americans Still Lack Retirement Savings*, Regional Economist (1st Qtr. 2018), available at: *https://www.stlouisfed.org/publications/regional-economist/first-quarter-2018/many-americans-still-lack-retirement-savings?print=true#1*.

Recent trends since the 1980s have given American workers more individual responsibility and control in retirement planning. During this period, companies shifted their worker retirement arrangements from defined benefits plans to defined contribution plans, such as 401(k) plans.[482] Defined contribution plans may be potentially better suited to an environment in which workers frequently change jobs,[483] while giving individuals greater responsibility for prudent investment of their retirement savings.

With respect to defined contribution and other self-directed retirement plans, individuals must decide when to start saving, how much to invest, which investments to select for an asset allocation that matches their risk tolerances, and what to do when transitioning between employers. Individuals may be ill-equipped to make these complex decisions, which can have significant consequences for their financial security in retirement.[484] According to one survey of individuals who had self-directed retirement savings, 53% were either not comfortable or were "only slightly comfortable making these decisions.[485] For 59% of workers, the survey found that it was their lack of interest or capacity for saving in a 401(k) plan that limited their participation, rather than their employer not providing a plan to invest in.[486]

Although providing 401(k) plan participants with advice would help them manage their accounts, a recent industry survey found that only a minority of plan sponsors were offering investment advice to plan participants.[487] In 2016, GAO reported that plan sponsors might be reluctant to provide this investment advice due to the costs and concerns of potential legal liability.[488]

Digital Tools

Digital financial planning brings the possibility of expanded access to advice for a larger number of Americans. Although personal finance software has been available since the early 1990s, these digital tools have become more sophisticated when combined with data aggregation. Through the use of data analytics, machine learning, and other computing advances, the costs of providing digital financial planning have declined significantly. Compared to human financial planners, digital financial planning services are often available to individuals with minimal balances.[489]

---

482. GAO Fintech Report, at 9.

483. Employee Benefits Research Institute, *Employee Tenure Trends, 1983-2016* (Sept. 17, 2017), at 3, available at: *https://www.ebri.org/pdf/notespdf/EBRI_Notes_v38no9_Tenure.20Sept17.pdf* (indicating that employee tenure data from the U.S. Census Bureau shows that the notion of a worker staying with the same employer for most of his or her career has never existed for most works and will continue not to exist).

484. U.S. Government Accountability Office, *The Nation's Retirement System: A Comprehensive Re-evaluation is Needed to Better Promote Future Retirement Security* (Oct. 2017), at 22, available at: *https://www.gao.gov/assets/690/687797.pdf*.

485. Board of Governors of the Federal Reserve System, *Report on the Economic Well-Being of U.S. Households in 2016* (May 2017), at 59, available at: *https://www.federalreserve.gov/publications/files/2016-report-economic-well-being-us-households-201705.pdf*.

486. Id. at 60.

487. Plan Sponsor Council of America, *60th Annual Survey of Profit Sharing and 401(k) Plans* (Feb. 2018) (finding that about one-third of plan sponsor respondents offer investment advice to participants).

488. U.S. Government Accountability Office, *401(k) Plans: DOL Could Take Steps to Improve Retirement Income Options for Plan Participants* (Aug. 2016), at 47, available at: *https://www.gao.gov/assets/680/678924.pdf*.

489. GAO Fintech Report, at 13-14.

Investment assets managed by digital advisers are projected to grow from $100 billion in 2017 to $385 billion by 2021.[490]

More importantly, digital financial planning is available to younger individuals who are entering the work force, a stage at which their wealth is typically quite small. Establishing a pattern of saving and investing during the early period of an individual's career can significantly increase the probability of long-term success in accumulating wealth and building retirement savings.[491]

Digital financial planning is currently offered directly to consumers via the Internet, and some services require little, if any, interaction with a human advisor. Other methods for providing digital financial advice may emerge in the future, such as through the use of chatbots.[492] These technological developments have resulted in certain market participants seeking to significantly undercut the pricing of human financial planners in an effort to attract clients and their assets.

At the same time, digital tools have altered the way traditional financial planners provide services to their clients. Data aggregators, for example, reduce the need of financial planners to engage in the menial task of compiling information from multiple client accounts, thereby freeing up time for more value-added activities.[493] For financial planners that are registered as brokers or investment advisers, data aggregation can be used to provide a more complete picture of a client's financial situation for purposes of suitability assessments or providing advice under a fiduciary standard.[494] Firms that employ human financial planners have reported that digital tools also improved the consistency of advice provided to clients.

Another model for providing financial planning services has also emerged. Referred to as the "hybrid" model, this model utilizes an internet or mobile-based interface for primary interaction with clients but also allows for contact with a human financial planner. Typically, fintech financial planning entities provide access to a human financial planner for an additional fee or with a higher-level service package.

Digital financial planning offers a wide range of services, some of which are more comprehensive than others. This is similar to how traditional firms market financial planning services, but may

---

490. Liz Skinner, *5 Robo-Advisers with the Most Client Assets*, Investment News (June 6, 2017), available at: *http://www.investmentnews.com/article/20170606/FREE/170539987/5-robo-advisers-with-the-most-client-assets* (citing a report from Cerulli Associates).

491. Employee Benefits Security Administration, U.S. Department of Labor, *New Employee Savings Tips – Time Is on Your Side*, available at: *https://www.dol.gov/sites/default/files/ebsa/about-ebsa/our-activities/resource-center/publications/new-employee-savings-tips-time-is-on-your-side.pdf* (last accessed July 10, 2018).

492. See, e.g., Sharon Adarlo, *Will Small Clients be Claimed by Chatbots?*, Financial Planning (Apr. 18, 2018), available at: *https://www.financial-planning.com/news/whats-the-word-on-chatbots-in-wealth-management?brief=00000153-6773-d15a-abd7-efff45d10000*.

493. See, e.g., Heidrick & Struggles, *Future of Digital Financial Advice* (Dec. 2016), at 19-20, available at: *https://centerforfinancialplanning.org/wp-content/uploads/2016/12/Future-of-Digital-Financial-Advice.pdf* (summarizing the work of the Certified Financial Planner Board of Standards Digital Advice Working Group).

494. Lowell Putnam, Quovo, *FINRA Standards Depend on Account Aggregation, Despite Alert's Caution*, blog post (Apr. 13, 2018), available at: *https://www.quovo.com/fintech-blog/the-ecosystem/finra-standards-depend-on-account-aggregation-despite-alerts-caution/*.

only offer limited advice.[495] Digital financial planning is offered by fintech applications, banks and brokerage firms, and technology companies. They often use the services of a data aggregator to centralize information about a consumer's accounts from multiple financial institutions.

The scope and nature of digital financial planning continue to evolve.[496] Digital financial planning services offer the ability to aggregate all accounts in one location and to produce balance sheet type information, such as net worth and investment portfolio summaries. Other services include budgeting, goal setting, and bill payment functions. Some tools compare a consumer's expenses and savings to peer groups in order to change the consumer's behavior, while others analyze spending patterns based on financial transaction data. Using computer algorithms, the service will make recommendations, such as to reduce expenses in particular areas or to consider re-financing outstanding debt. Some services automatically send funds to investment accounts, such as by rounding up spending transactions or diverting anticipated savings.

Digital financial planning can offer advice with respect to securities, loan products, or insurance products. Computer algorithms can provide advice that recommends an asset allocation and portfolio investments based on the consumer's responses to questions regarding risk tolerance, time horizons, and other factors. Some services provide exposure to recommended asset classes through investment vehicles like low-cost, exchange-traded funds. Investment portfolios may be automatically rebalanced to remain within recommended allocations and receive advice on tax loss harvesting strategies.

Some digital financial planning services directly charge consumers, through either a fixed-fee or a percentage of assets under management. Other programs offer a limited set of services for free and allow the consumer to "buy up" for additional services. Some services do not impose any fee directly on the consumer, but instead have relationships with financial partners that pay a fee for inclusion in the range of products that the service may recommend.

Issues and Recommendations

Financial planning has not been directly regulated by the federal or state governments through licensing or registration requirements.[497] Instead, regulatory oversight is triggered either by engaging in certain activities as part of offering financial planning services or by offering these services by an individual who is regulated under another regime.

---

495. Financial Planning Coalition, *Consumers Are Confused and Harmed: The Case for Regulation of Financial Planners*, White Paper (Oct. 2014), at 16-19, available at: *http://financialplanningcoalition.com/wp-content/uploads/2014/06/Financial-Planning-Coalition-Regulatory-Standards-White-Paper-Final.pdf* ("FPC White Paper").

496. Cf. Michael Kitces, *The Six Levels of Account Aggregation #FinTech and PFM Portals for Financial Advisors*, blog post (Oct. 9, 2017), available at: *https://www.kitces.com/blog/six-levels-account-aggregation-pfm-fintech-solutions-accounts-advice-automation/*.

497. Some states have adopted laws regulating the conduct of financial planners, but they do not require licensing or registration as a financial planner. The definition of a financial planner under state law can vary. For example, Nevada's law applies only to persons offering advice for compensation "upon the investment of money or upon provision for income to be needed in the future" but Minnesota's law applies to any person "engaged in the business of financial planning." See Nev. Rev. Stat. § 628A; Minn. Stat. § 45.026. Both the Minnesota and Nevada laws impose a fiduciary duty upon financial planners, but, for example, Connecticut only requires disclosure of whether a financial planner has a fiduciary duty. See Conn. Pub. Act No. 17-120 (July 5, 2017).

Many financial planners provide investment advice and are therefore regulated by the SEC or state securities regulators.[498] Securities regulators have responded to the recent rise in digital investment advice by providing guidance related to compliance obligations under existing laws and regulations.[499] Securities regulators also have antifraud authority for nonsecurities advice that stems from the advisory relationship.[500]

Financial planning services provided by agents in connection with the sale of insurance products are regulated by state insurance regulators. Financial planners providing advice to plan participants in 401(k) plans are also subject to the obligations and prohibitions under Employee Retirement Income Security Act of 1974 and DOL rules. Although the Bureau has the authority to regulate consumer financial products or services, including financial advisory services (other than services relating to securities provided by a person regulated by the SEC or a state securities regulator, and who is acting in a regulated capacity) provided to consumers for individual financial matters or relating to proprietary financial products or services,[501] the Bureau generally does not have authority over accountants, tax preparers, and attorneys.[502]

Financial planning activities conducted by banks and its employees are subject to supervision by bank regulators and the Bureau. Accountants and attorneys offer financial planning services that are subject to oversight by state boards of accountancy and state bars, which may include regulation for conflicts of interest.

Under the current regulatory structure, financial planners could be subject to regulation by multiple regulators at the federal and state levels, with each regulator responsible for the specific activities falling within that regulator's purview. Treasury has concerns as to whether the current regulatory structure is efficient and appropriately rationalized. For example, a number of digital financial planning tools do not provide advice on 401(k) accounts, and some participants in outreach discussions indicated that regulatory compliance concerns were a factor in such decisions. Given that 401(k) account balances may account for a significant portion of an individual's investment portfolio, the lack of advice on such accounts will not advance Americans' ability to save for retirement and accumulate wealth.

---

498. Applicability of the Investment Advisers Act to Financial Planners, Pension Consultants, and Other Persons Who Provide Investment Advisory Services as a Component of Other Financial Services (Oct. 8, 1987) [52 Fed. Reg. 38400 (Oct. 16, 1987)].

499. See Division of Investment Management, U.S. Securities and Exchange Commission, *IM Guidance Update 2017-12: Robo-Advisers* (Feb. 2017), available at: *https://www.sec.gov/investment/im-guidance-2017-02.pdf*; Financial Industry Regulatory Authority, *Report on Digital Investment Advice* (Mar. 2016), available at: *https://www.finra.org/sites/default/files/digital-investment-advice-report.pdf*.

500. Under the antifraud provisions of the Investment Advisers Act, there is no requirement that fraudulent behavior by an investment adviser be in connection with the purchase or sale of securities. See 15 U.S.C. § 80b-6(1) and (2).

501. 12 U.S.C. §§ 5481(15)(A)(viii) and 5491(a). A financial product or service does not include activities relating to the writing of insurance. See 12 U.S.C. § 5481(15)(C).

502. 12 U.S.C. § 5517.

Recommendations

Numerous approaches could be undertaken to rationalize the regulatory framework for financial planning. For instance, one could focus regulatory responsibility exclusively within a single federal regulator, either new or existing. Another could be to create a self-regulatory organization (SRO) that would be subject to oversight by one or more federal regulators. The SRO could be responsible for promulgating rules, conducting inspections, and undertaking enforcement, as there are currently no widely applicable regulatory standards for those offering, or claiming to offer, financial planning advice that include competency standards and standards of conduct.[503] Alternatively, the SRO could only promulgate rules, and rely on a regulator to carry out examination and enforcement.

Treasury believes that appropriate protection for clients of financial planners, digital and otherwise, can be achieved without imposing either a fragmented regulatory structure or creating new regulatory entities. Treasury has concerns that the current regulatory structure discourages the provision of integrated investment advice for assets held in retirement and nonretirement accounts. A patchwork of regulatory authority makes it more costly for financial planners — costs that will be passed on to consumers in the form of higher costs or reduced services. The fragmented regulatory structure also potentially presents unnecessary barriers to the development of digital financial planning services.

Treasury recommends that an appropriate existing regulator of a financial planner, whether federal or state, be tasked as the primary regulator with oversight of that financial planner and other regulators should exercise regulatory and enforcement deference to the primary regulator. To the extent that the financial planner is providing investment advice, the relevant regulator will likely be the SEC or a state securities regulator.

503. FPC White Paper, at 12-15.

Enabling the Policy Environment

Agile and Effective Regulation for a 21st Century Economy

Introduction

While the financial services industry has been a frequent adopter of new technology, the current scale and pace of technological change has left many regulators re-examining their regulatory frameworks for shortcomings from a perspective of both regulatory efficiency and effectiveness.

The United States has historically led the world in innovation in financial services. Innovation has played a factor in making the U.S. capital markets the largest, deepest, and most vibrant in the world and has been of critical importance in supporting the U.S. economy. But the United States cannot take its leading position in innovation for granted. As the rest of the world takes measures to improve its ability to create, develop, and deploy innovative new products and services in the financial sector, the United States risks losing out by failing to provide appropriate regulatory clarity and assurances, and remove unnecessary barriers to innovation.

> The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed. New technologies include advanced computing, "big data" analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology – the very technologies that ensure we will be able to fight and win the wars of the future.
>
> *The Honorable James N. Mattis, Secretary of Defense*[504]

Regulatory Sandboxes

Competitive and free markets help foster economic growth. New ideas can facilitate market efficiency, spurring improvements to services and products. Not all innovations will succeed; some might even cause harm. Regulation should address and potentially mitigate negative externalities. A regulatory environment with largely binary outcomes — either approval or disapproval — may lack appropriate flexibility for dealing with innovations and often results in extensive delays, after which the innovation has become obsolete.

The regulatory environment should instead be flexible so that firms can experiment without the threat of enforcement actions that would imperil the existence of a firm. Innovating is an iterative process, and regulator feedback can play a helpful role while upholding safeguards and standards.

504. Secretary Jim Mattis, *Summary of the 2018 National Defense Strategy of the United States of America*, available at: *https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf*.

Treasury recognizes that U.S. regulators already employ a number of methods in support of innovation and encourages them to build on their efforts. Some examples include:

- Outreach efforts conducted throughout the United States to meet with innovators
- Creation of an agency innovation office so that innovators have a central point of contact
- Issuance of guidance, exemptive orders, or no-action letters, which may have conditions or be time-limited, to permit experimentation in the marketplace
- Agency-wide working groups that span multiple divisions and offices to address new technology trends
- Publication of white papers, speeches, and other materials discussing innovations and technology
- Engagement with foreign regulators on new developments, including cross-border collaboration agreements

During outreach discussions with Treasury, however, many stakeholders expressed frustration with the sheer number of agencies at the federal and state levels that need to be consulted when bringing a new product or service to market. Frequently, firms find that it is not even clear which agencies — or which units within those agencies — need to be engaged. The result is that innovators, particularly smaller firms, face significant and unnecessary burdens in terms of time, money, and opportunity costs.

The fragmented nature of the U.S. financial regulatory system undercuts efforts by regulators to support innovation. For example, a no-action letter or exemptive relief from one agency may be of limited use without assurance that other agencies with jurisdiction will provide comparable relief. Fragmentation also raises the likelihood of inconsistency among regulators. To be effective, a coordinated effort is needed to obtain appropriate relief across the marketplace.

New technologies, like predictive data analytics, artificial intelligence, and blockchain or distributed ledger technology, are examples of promising innovations that could be used by financial services firms. They are also technologies for which regulatory treatment may be uncertain, if for no other reason than that innovative technology requires time to mature. From the perspective of regulators, these technologies may pose unknown benefits and risks. In such situations, it would be beneficial for regulators to permit meaningful experimentation in the real world, subject to appropriate limitations.

Recommendations

Treasury recommends that federal and state financial regulators establish a unified solution that coordinates and expedites regulatory relief under applicable laws and regulations to permit meaningful experimentation for innovative products, services, and processes. Such efforts would form, in essence, a "regulatory sandbox" that can enhance and promote innovation. The solution should be based on the following principles:

- Promote the adoption and growth of innovation and technological transformation in financial services
- Provide equal access to companies in various stages of the business lifecycle (e.g., start-ups and incumbents)

- Delineate clear and public processes and procedures, including a process by which firms enter and exit
- Provide targeted relief across multiple regulatory frameworks
- Offer the ability to achieve international regulatory cooperation or appropriate deference where applicable
- Maintain financial integrity, consumer protections, and investor protections commensurate with the scope of the project
- Increase the timeliness of regulator feedback offered throughout the product or service development lifecycle

Treasury will work with federal and state financial regulators to design such a solution in a timely manner. The alternative of establishing a formal sandbox overseen by a single regulator would require preemption of a firm's other regulators, and in some cases may even subject a firm to a new regulator that is unfamiliar with its operations; it is also very unclear who that single regulator would be. If financial regulators are unable to address these objectives, however, Treasury recommends that Congress consider legislation to provide for a single process consistent with the principles set forth above, including preemption of state laws if necessary.

The parameters of any regulatory sandbox should be designed with the participation of the private sector and contain appropriate metrics for testing, including sample size and development periods appropriate to these endeavors, to ensure the effectiveness of product and service development.

International Efforts in Financial Technology

The ongoing attempt to balance innovation and regulation has spawned new regulatory initiatives, public-private partnerships, and investment schemes across both developed and emerging economies. In an effort to drive innovation, domestic investment, and effective new regulatory approaches, financial authorities abroad have endeavored to establish various "innovation facilitators." In a recent survey by the Financial Stability Board and Basel Committee on Banking Supervision, authorities provided information about their respective domestic approaches toward innovation facilitators in three distinct categories: innovation hubs, accelerators, and regulatory sandboxes.[505] Innovation hubs such as LabCFTC provide access points to regulators for fintech firms, which has the dual benefit of providing firms more regulatory clarity and facilitating information sharing with regulators. Accelerators, such as the various grants and schemes in Singapore's Startup SG ecosystem, offer firms incentives to innovate and start businesses. Regulatory sandboxes like Hong Kong's Fintech Supervisory Sandbox provide an environment for firms to conduct pilot trials of financial innovations under lower regulatory burdens than might traditionally be required for the same service provided in a different way, while offering the authorities insights and feedback on new approaches.

505. Basel Committee on Banking Supervision, *Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors* (Feb. 2018), available at: *https://www.bis.org/bcbs/publ/d431.pdf*.

Sandbox Case Studies

Monetary Authority of Singapore

The Monetary Authority of Singapore (MAS) has introduced a regulatory sandbox — a policy framework that relaxes specific legal and regulatory requirements for a fixed time period for fintech and financial institutions experimenting with innovative products and services. Firms apply for entry into the sandbox, and if approved, MAS will determine what specific regulations it is prepared to relax for participating firms. In its guidelines for the regulatory sandbox, MAS notes that the sandbox is not meant to help firms circumvent legal and regulatory requirements, but is instead meant to help encourage efficiency and manage risks in the financial sector.[506] The sandbox may not be appropriate, for instance, if the proposed innovation is similar to a service already being offered in Singapore or if the applicant has not demonstrated an adequate level of due diligence. The guidelines are also clear that the financial service should have a clear plan to deploy in Singapore or be able to provide some benefit for Singapore's market and consumers. If a firm is successful in its experimentation, then upon exiting the sandbox, it must fully comply with Singapore's legal and regulatory requirements. The MAS sandbox accepts applications at any time and, if needed, MAS will permit firms to extend their time in the sandbox on a case-by-case basis.

United Kingdom Financial Conduct Authority

The U.K. Financial Conduct Authority (FCA) launched a regulatory sandbox in June 2016 as part of the FCA's Project Innovate, an initiative started in 2014 to encourage innovation with an explicit mandate to promote competition in U.K. financial services.[507] The FCA selects firms in cohorts regardless of a firm's size or maturity, and allows these firms to test within the sandbox on a small scale while providing a degree of regulatory clarity and guidance. Firms in the sandbox are assigned a dedicated case officer and may be provided with targeted regulatory assistance, such as waivers or no-action letters, to facilitate a customized regulatory environment for each test. Before testing in the sandbox, however, firms must meet authorization requirements relevant for the proposed activity and must meet sufficient, bespoke safeguards to mitigate consumer harm. Upon transitioning out of the sandbox, firms are required to submit a final report highlighting the outcomes of the test. The FCA has also indicated an interest in establishing a global sandbox, where firms could potentially participate and conduct tests spanning more than one jurisdiction.

Agile Regulation

The pace of technological development and its applications to financial services have increased dramatically. It is critical that financial regulators stay abreast of developments and establish mechanisms for adopting appropriate regulation and guidance accordingly without stifling innovations

506. Monetary Authority of Singapore, *Fintech Regulatory Sandbox Guidelines* (Nov. 2016), available at: *http://www.mas.gov.sg/~/media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines%2019Feb2018.pdf*.

507. Financial Conduct Authority, *Regulatory Sandbox Lessons Learned Report* (Oct. 2017), available at: *https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf*.

that require time to mature. Regulators must be more agile than in the past in order to successfully uphold their missions without creating unnecessary barriers to innovation. This requires principles- and performance-based regulation that enables the private sector to adopt innovative, technology-based compliance solutions.

In addition, regulators need to understand technology on the same timeline as business. To do this, financial regulators need to engage with the private sector to test and understand new technologies and innovations as they arise. Agile regulation requires regulators to acquire and understand existing and emerging technologies, to engage with developers and first-movers, and to hire and retain staff with the appropriate technical expertise. To this end, Treasury believes that regulators should increase efforts to proactively engage in collaborative dialogue with the private sector as innovations arise. Regulators should be looking to facilitate U.S. strengths in technology and work toward the common goals of fostering markets and promoting growth through responsible innovation.

Procurement

As new technologies are introduced in the financial services sector, financial regulators require the ability to work interactively with them in order to understand them, determine potential regulatory or operational implications, and evaluate them for potential use by the regulator itself. Regulators' hands, however, are frequently tied when it comes to obtaining such technology. Although innovators and other participants are often willing to provide the technology or proofs of concept to the regulator to help improve their understanding, statutory and regulatory requirements can either expressly prohibit, or effectively prohibit, the acquisition of the technology as either a gift or a purchase.

Under principles of federal appropriations law, federal agencies may not augment their appropriations from outside sources absent specific statutory authority.[508] Whether an agency may accept goods and services often depends on whether the agency has statutory authority to accept gifts. Because of the longstanding principle against augmenting appropriations, federal agencies may not accept for their own use gifts of money or other property in the absence of specific statutory authority.[509] Thus, even though many fintech companies are willing to provide regulators with new technology at no cost in order to demonstrate viability or to help expedite the regulatory process, federal regulators may be precluded from accepting such offers.

If a federal financial regulator wants to purchase a particular technology and has appropriated funds, federal acquisition regulations can make it difficult to do so in a timely enough manner to justify the purchase. For example, procurement regulations generally require an agency to first establish a defined need for the acquisition, describe the requirements to satisfy the agency need, and then either engage in sealed bidding or competitive negotiation, which can take many months. In outreach meetings with Treasury, some regulators indicated that it can be difficult to identify a specific agency need or describe exact requirements for a potential technological solution requiring incubation, and that, even if they could, the time to complete the acquisition would

508. U.S. Government Accountability Office, *Principles of Federal Appropriations Law, Volume II* (3rd ed. Feb 2006), at 6-162, available at: *https://www.gao.gov/assets/210/202819.pdf*.

509. Id. at 6-222.

be too lengthy to be effective. The nature of innovative new technologies — not yet widespread, often without direct substitutes, and materially advancing in technology in matters of weeks not months — does not fit the traditional competitive bidding and procurement processes set out by federal acquisition regulations. Even the process a firm must undergo to be considered an eligible bidder for a government contract often dissuades firms from entering the bidder pool, particularly younger companies with less resources and newer technologies that are bound to change before the process is completed. These challenges significantly limit some financial regulators' ability to better understand, test, and procure new technologies, potentially constraining the effectiveness and efficiency of federal regulation.

Federal acquisition law establishes "other transaction authority," which allows select government agencies to develop agreements that do not need to adhere to a standard format or include terms and conditions required in traditional approaches to acquisition.[510] Other transaction authority has been authorized for the U.S. Department of Defense (DOD), U.S. Department of Energy, U.S. Department of Health and Human Services, U.S. Department of Homeland Security (DHS), U.S. Department of Transportation, National Aeronautics and Space Administration, Federal Aviation Administration, Transportation Security Administration, Domestic Nuclear Detection Office, Advanced Research Projects Agency-Energy, and certain programs at the National Institutes of Health. Other transaction authority can be granted on a permanent or temporary basis.

Other transaction authority has been used by these agencies to facilitate critical understanding and application of new technology by the government. DOD launched the Defense Innovation Unit (Experimental) (DIUx) in order to accelerate the development, procurement, and integration of commercially derived disruptive capabilities.[511] As DIUx has noted, the state of innovation is "dramatically different from past decades when key technologies were developed in government labs," with many new technological developments originating from the commercial sector.[512] Since June 2016, DIUx has initiated 61 prototype projects with an average time of only 90 days from first contact to contract award.[513] Similarly, using other transaction authority, DHS established its Next Generation Cyber Infrastructure Apex program ("Cyber Apex"), which seeks out solutions to fill cybersecurity gaps and protection of critical systems and networks.[514] Cyber Apex is working with a consortium, which includes private companies in the financial services sector, to test existing marketplace solutions, while simultaneously working with a DHS innovation program in Silicon Valley in search of early-stage solutions.[515]

---

510. U.S. Government Accountability Office, *Federal Acquisitions: Use of "Other Transaction" Agreements Limited and Mostly for Research and Development* (Jan. 2016), available at: *https://www.gao.gov/assets/680/674534.pdf*.

511. Defense Innovation Unit (Experimental), U.S. Department of Defense, *Commercial Solutions Opening (CSO)*, at 1, available at: *https://www.diux.mil/download/datasets/736/DIUx-Commercial-Solutions-Opening-White-Paper.pdf* (last accessed June 29, 2018).

512. Defense Innovation Unit (Experimental), U.S. Department of Defense, *Annual Report 2017*, at 2, available at: *https://www.diux.mil/download/datasets/1774/DIUx%20Annual%20Report%202017.pdf.*

513. Id. at 4.

514. Cyber Security Division, U.S. Department of Homeland Security, *Technology Guide 2018*, at 6, available at: *https://www.hsdl.org/?view&did=808790*.

515. Id.

Recommendations

Treasury recommends that Congress enact legislation authorizing financial regulators to use other transaction authority for research and development and proof-of-concept technology projects. Regulators should use this authority to engage with the private sector to better understand new technologies and innovations and their implications for market participants, and to carry out their regulatory responsibilities more effectively and efficiently. Using the expertise of the private sector in developing regulatory tools will generally produce more optimal solutions than restricting input to be entirely in-house.

Regtech

In the aftermath of the financial crisis, financial services companies have incurred increased compliance costs in an environment of enhanced regulatory scrutiny. This dynamic has led to the rise of firms specifically focused on delivering products and services that assist regulated entities in meeting compliance requirements. These firms have been labeled by some as "reg-tech" companies.

Regtech within financial services has grown rapidly as advances in technology have made it possible to deliver automated solutions for compliance tasks that are otherwise performed manually. Estimates suggest there are some 80-250 firms currently operating that primarily serve the financial services industry's compliance and regulatory needs. The range of services is broad and includes activities such as customer identification/verification and transaction monitoring for Bank Secrecy Act anti-money laundering/countering the financing of terrorism; antifraud surveillance; risk assessment and management; market conduct services; origination processes; and regulatory requirement monitoring.[516]

Financial services companies may benefit from partnering with regtech firms that have proprietary technologies or processes such companies may not be able to build in-house, particularly smaller entities, such as community banks, that may not have the financial resources to develop internally the technologies necessary to achieve marginal reductions in risk and compliance costs. One report on regtech firms estimates that "governance, risk and compliance (GRC) costs account for 15% to 20% of the total 'run the bank' cost base of most major banks. GRC demand drives roughly 40% of costs for 'change the bank' projects under way."[517]

Regulators at both the federal and state levels can have a significant impact on the regtech industry through not only the compliance requirements they set, but also the means by which examination for compliance is executed. Some emerging regtech solutions aim to facilitate more efficient communication between regulated financial institutions and regulators by providing APIs or distributed ledger technology-based channels to share information, such

516. See Bain and Company, *Banking Regtechs to the Rescue?* (2016), available at: *http://www.bain.com/Images/BAIN_BRIEF_Banking_Regtechs_to_the_Rescue.pdf*; and PricewaterhouseCoopers, *Regtech in Financial Services (2018)*, available at: *https://www.pwc.com/us/en/industries/financial-services/research-institute/top-issues/regtech.html*.

517. See Bain and Company, at 3.

as suspicious transaction reports and supporting information, or other mandatory reports, with central banks and regulators, and by providing digital channels for further inquiries and responses.

Treasury encourages regulators to appropriately tailor regulations to ensure innovative technology companies providing tools to regulated financial services companies can continue to drive technological efficiencies and cost reductions. Additionally, Treasury encourages regulators to seek out and explore innovative partnerships with financial services companies and regtech firms alike to better understand new technologies that have the potential to improve the execution of their own regulatory responsibilities more effectively and efficiently.

Engagement

Beyond experimentation, broad regulatory engagement with financial services companies on multiple levels is essential. Treasury commends the efforts by financial regulators to create labs, working groups, innovation offices, and other channels for industry participants to engage directly with regulators. These discussions provide regulators with visibility into technology developments and provide an opportunity to receive real-time feedback from regulators on their ideas. Additionally, they encourage an ongoing dialogue, lessening the likelihood that financial services firms are operating based on erroneous information or misinterpretation of regulations.

However, a number of reasons have been provided for why some in the private sector may be reluctant to communicate openly with regulators. A few participants in Treasury outreach meetings raised concerns that conversations with regulators could be used as a reason to initiate an enforcement investigation.[518] Participants argued that if regulators are not in a position during engagement sessions to provide either assurances or helpful advice on how innovations can comply with the rules, then there is little for the market participant to gain from a one-way engagement and significant risk of being delayed and losing the chance to be the first to market. Some firms faulted financial regulators for having an "enforcement first" perspective, not being timely in providing useful guidance, and not having a sufficient appreciation of how delay and regulatory uncertainty can result in a new product or service being overtaken by a competitor.

Recommendations

Treasury recommends that financial regulators pursue robust engagement efforts with industry and establish clear points of contact for industry and consumer outreach. The outcome of engagement should be to create an environment where growth can occur with appropriate protections while reducing compliance costs. Both regulators and the private sector must recognize that they have a symbiotic relationship that is needed to support the U.S. economy and maintain global competitiveness.

Treasury recommends that financial regulators increase their efforts to bridge the gap between regulators and start-ups, including efforts to engage in different parts of the country rather than

518. On the other hand, Treasury acknowledges that some firms may have had reason to believe that their activities might be subject to regulation and chose not to bring their activities to the attention of regulators. See, e.g., Peter Van Valkenburgh, Coin Center, *Framework for Securities Regulation of Cryptocurrencies* (Jan. 2016), available at: *https://coincenter.org/wp-content/uploads/2016/01/SECFramework2.5.pdf* (noting that some cryptocurrencies may "functionally resemble securities" when sold to investors).

requiring entities to come to Washington, D.C. Unlike incumbent financial institutions with well-established government relations offices, start-ups may be less familiar with how to engage with federal regulators but equally critical for regulators to engage with. While start-ups must comply with existing laws and regulations, regulators should seek to understand the business models of these entities that may be subject to their authorities. Further, Treasury recommends that financial regulators periodically review existing regulations as innovations occur and new technology is developed and determine whether their regulations fulfill their original purpose in the least costly manner.

Treasury recommends that financial regulators engage at both the domestic and international levels, as financial technology in many cases is borderless. Treasury encourages international initiatives by financial regulators to increase their knowledge of fintech developments in other nations, such as the recent agreement between the CFTC and the U.K. Financial Conduct Authority.[519]

Education

More efforts need to be taken to close the knowledge gap, both between private industry and regulators, and among and within financial regulators themselves. In outreach meetings with Treasury, many industry participants from both the financial services industry and the technology industry indicated that regulators and examiners often lack basic knowledge about the technologies employed by firms. Participants also indicated that technical sophistication often varied among regulators, adding to difficulties in navigating an already fragmented regulatory system.

Treasury acknowledges that it is challenging for the U.S. government to attract and retain talented human capital, as it lacks the ability to compete for such talent with incentives such as higher salaries and equity compensation. While the attraction of highly qualified technical personnel to the private sector may disadvantage the government, it is surely a benefit for U.S. firms leading the world in innovation.

Because innovation in technology occurs at such a rapid pace, Treasury recognizes that it may be impractical for individuals to leave the private sector temporarily and commit to public service for an extended period of time without being at significant risk of not being able to re-enter the technology sector at a competitive level. Thus, the nature of the technology industry creates a structural close hold on its workforce. Despite these differences, Treasury believes that a number of steps can be taken to improve the technology-savviness of the regulatory workforce.

Currently, some universities have programs that bring policymakers and the technology industry together through practical simulations and experiential learning, requiring each to walk in the shoes of the other. These activities, for instance when applied to topics like cybersecurity, help policymakers to understand and appreciate the demands of managing a corporation and a firm's duties that may cause the firm to take various actions in response to regulatory guidance. These types of experiential learning opportunities are critical to bridging the knowledge gap between regulators and the entities they regulate.

519. U.S. Commodity Futures Trading Commission, *Press Release No. 7698-18* (Feb. 19, 2018), available at: *https://www.cftc.gov/PressRoom/PressReleases/pr7698-18*.

Another approach to bridging this gap is to bring experts into a regulatory agency on temporary assignment. Some agencies, like the SEC, already have existing professional fellowship programs in which outside industry veterans join the agency on a non-permanent basis and are subject to extensive requirements to manage any conflicts of interest that arise from their temporary hiatus from the private sector. Regulators benefit from exposure to the fellow's knowledge, and the fellow benefits from exposure to the regulator's mission and operations. The experience and understanding of regulatory processes acquired during these fellowships is then shared by the participating fellows upon returning to industry.

Since 2012, the U.S. Government has recruited Presidential Innovation Fellows to leverage outside industry expertise to work with the government. The Presidential Innovation Fellows serve for a 12-month program, which can be extended for up to a total of four years. To date, none of the financial regulators have participated in the program. Recently, the OCC considered creating new positions for Innovation Fellows as part of its efforts to better understand innovation. Treasury encourages financial regulators to consider establishing similar fellowship opportunities that would focus on financial technology, recognizing the likely shorter duration required to make such a fellowship successful in attracting the right talent.

Critical Infrastructure

The transformational technologies and service offerings examined by this report in key areas of financial services have generated even further innovation leading to the re-architecting of current technologies, applications, networks, and back-office infrastructures. Cybersecurity, resilience, and operational risk considerations are inseparable from any examination of these technologies. Particularly when applied to financial services, these developments directly impact the nation's critical infrastructure.

Increased reliance on emerging technologies yields benefits as well as new risks, requiring developers to build for security, resiliency, and agility from the start, not as afterthoughts. Treasury recommends that financial regulators thoroughly consider cybersecurity and other operational risks as new technologies are implemented, firms become increasingly interconnected, and consumer data are shared among a growing number of firms, including third parties. The task of ensuring that the country's critical infrastructure — systems, networks, functions, and data — remain available and reliable is increasingly complex as risks may reside throughout the supply chain, not solely with the owner or operator. Furthermore, the supply chain includes a mix of firms, operating under a range of cybersecurity risk profiles — some may lack common baseline cybersecurity protections and standards, and others, even regulated firms subject to cybersecurity regulations, suffer from differing interpretations and implementations of regulatory guidance. A firm with a more mature cybersecurity posture may additionally be exposed to cybersecurity risks because its vendors or suppliers have not developed a similarly robust cybersecurity posture.

The Banking Report provided two recommendations regarding cybersecurity that Treasury continues to endorse: (1) developing a common lexicon, and (2) harmonizing regulations.[520] In addition to the work taking place within the Financial and Banking Information Infrastructure Committee (FBIIC) to implement those recommendations, the FBIIC agencies should neither stifle innovation, nor mandate specific technology solutions; the FBIIC agencies should remain technology neutral. Treasury additionally recommends that the FBIIC consider establishing a technology working group charged with better understanding the technologies that firms are increasingly relying upon, and staying well-informed regarding innovation taking place within the sector.

Policy approaches to protect the nation's critical infrastructure cannot focus solely on regulation and the financial regulators. Treasury will continue to partner with federal agencies to better understand supply chain and third-party risks, and work directly with financial services firms, and across the critical infrastructure community, to address these challenges.

Treasury also encourages the sector to migrate away from the historical focus on threat, and balance that with a focus on vulnerability identification and remediation. Broadly speaking, the financial services industry works very hard now to identify threats that exploit vulnerabilities to create risk. Reducing vulnerabilities is as important, if not more so, as reducing risk. When a vulnerability is found and closed, no one can exploit it. Alternatively, finding one threat (such as a criminal enterprise) and shutting it down will still leave the vulnerability available in a system for exploitation by other threats.

To this end, Treasury commits to leading a multiyear program with the financial services industry to identify, properly protect, and remediate vulnerabilities. Finally, Treasury supports the industry's continued efforts to promote and support the adoption of the National Institute of Standards and Technology Cybersecurity Framework to reduce risks to the nation's financial critical infrastructure.

International Approaches and Considerations

Overview

Across the world, many economies are shifting toward enabling more open and faster banking services by enabling greater competition from nonbanks like fintechs and technology companies. Primarily, open banking has entailed enabling greater access to financial data or payment clearing and settlement systems that were previously maintained by or provided to banks and unavailable to nonbanks. Often, this enhanced access is provided through APIs. These efforts are largely in the preliminary stages of being implemented but are expected to significantly shape how financial services are delivered in these economies.

520. The Banking Report, at 31.

- India: India introduced the Unified Payments Interface (UPI) in August 2016, which allows for open API interfaces for real-time payments.[521] The UPI, combined with other policy efforts to minimize the use of cash, promote digital identity, and leverage mobile devices, has created an environment where many new payment players are expected to emerge.
- Europe and the United Kingdom: The Revised Payment Services Directive (PSD2) and the United Kingdom's Open Banking initiative were intended to encourage greater competition within these jurisdictions' banking systems by allowing nonbank firms to connect to banking payments and data systems through licensing regimes tailored for these activities.[522]
- Australia: Australia commissioned an open banking study, with the final report published in late 2017.[523] The government is now consulting on a final decision and implementation.
- Hong Kong: Hong Kong is embarking on an initiative to launch a "new era of smart banking." This initiative was announced in September 2017,[524] and includes areas of focus such as faster payments, fintech sandboxes, and open-banking APIs. To implement the API aspect of the strategy, the Hong Kong Monetary Authority published an open API framework in July 2018.[525]
- Singapore: The Monetary Authority of Singapore has taken a more organic approach to open banking. While the idea is being encouraged by the government, Singapore believes that open banking will ultimately be more successful if it is led by the industry and not done through government mandates.[526] Financial services companies have been working toward APIs as the Association of Banks in Singapore released a voluntary API playbook for banks in 2016.[527]

---

521. National Payments Corporation of India, *Press Release – NPCI's Unified Payments Interface (UPI) Set to Go Live* (Aug. 25, 2016), available at: *https://www.npci.org.in/sites/default/files/NPCIsUnifiedPaymentsInterface%28UPI%29settogoliveAugust252018.pdf*.

522. Competition and Markets Authority, *Retail Banking Market Investigation: Final Report* (Aug. 9, 2016), at 441-461, available at: *https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf*; Directive (EU) 2015/2366 of the European Parliament and of the Council (Nov. 25, 2015), available at: *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN* (preamble).

523. The Treasury (Australia), *Review into Open Banking: Give Customers Choice, Convenience and Confidence* (Dec. 2017), available at: *https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf*.

524. Hong Kong Monetary Authority, *Press Release – A New Era of Smart Banking*, Press Release (Sept. 29, 2017), available at: *http://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170929-3.shtml*.

525. Hong Kong Monetary Authority, *Press Release – Open API Framework for the Banking Sector and the Launch of Open API on HKMA's Website*, Press Release (July 18, 2018), available at: *http://www.hkma.gov.hk/eng/key-information/press-releases/2018/20180718-5.shtml*.

526. Chanyaporn Chanjaroen and Haslinda Amin, *Singapore Favors 'Organic' Policy in Move Toward Open Banking*, Bloomberg (Apr. 11, 2018), available at: *https://www.bloomberg.com/news/articles/2018-04-12/singapore-favors-organic-policy-in-move-toward-open-banking*.

527. The Association of Banks in Singapore, *Media Release – The Association of Banks in Singapore Issues Finance-as-a-Service: API Playbook*, Media Release (Nov. 16, 2016), available at: *https://abs.org.sg/docs/library/mediarelease_20161116.pdf*.

Within banking systems, there are also significant efforts to modernize and increase core capabilities, such as in the area of payments. Many jurisdictions around the world have embarked on initiatives to increase the speed of wholesale payments through implementation of real-time payment systems. As of mid-year 2017, it was estimated that there were 25 countries (primarily large advanced economies) that had some type of live faster-payments system.[528]

Impacting the provision of credit, nonbank digital lenders have emerged in many jurisdictions that deploy automated lending platforms, provide rapid credit decisions, and are funded through investment capital or peer-to-peer financing.[529] Some of the most sizable activity and fastest growth has occurred in U.S., Chinese, and U.K. markets. The U.S. market has grown rapidly to about $35 billion in 2016, or roughly three times 2014 levels. The U.K. market, while materially smaller, has also roughly tripled since 2014 to £4.6 billion. Meanwhile, the Chinese market has grown to $246 billion in 2016, up by a factor of 10 from $24.3 billion in 2014.[530] Common across these markets is an emphasis on providing credit to consumer and small business segments.

Data Regulation

The expanded access to financial and nonfinancial data enabled by movement toward more open banking across multiple jurisdictions has raised critical issues with respect to protecting the confidentiality of consumers' financial and personal data. Multiple jurisdictions have adopted laws to address some of these growing concerns with respect to their personal data. For example, Europe recently introduced its General Data Protection Regulation (GDPR), which attempts to create a fundamental right to privacy that includes the right for people to have their data deleted and transferred, among other provisions. The GDPR, however, has raised a number of questions about implementation for companies, regardless of their country of domicile, that hold the personal data of E.U. and U.K. citizens.[531] Uncertainties in the implementation of GDPR may also create unnecessary barriers to trade and damage cross-border regulatory cooperation due to this lack of regulatory clarity. Some other examples of efforts to add personal data protection regulations

528. FIS, *Flavors of Fast: A Trip Around the World of Immediate Payments* (4th ed. June 2017), at 29-55, available at: *https://www.fisglobal.com/flavors-of-fast-2017*.

529. See, e.g., World Economic Forum, *The Future of FinTech: A Paradigm Shift in Small Business Finance* (Oct. 2015), available at: *http://www3.weforum.org/docs/IP/2015/FS/GAC15_The_Future_of_FinTech_Paradigm_Shift_Small_Business_Finance_report_2015.pdf* (discussing small business lending via marketplace lenders).

530. Tania Ziegler et al., *The 2017 Americas Alternative Finance Industry Report*, University of Cambridge Judge Business School Centre for Alternative Finance (May 2017), available at: *https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-06-americas-alternative-finance-industry-report.pdf* (U.S. market); Kieran Garvey et al., *Cultivating Growth: The 2nd Asia Pacific Region Alternative Finance Industry Report*, University of Cambridge Judge Business School Centre for Alternative Finance (Sept. 2017), available at: *https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-12-cultivating-growth.pdf* (Chinese market); Bryan Zhang et al., *Entrenching Innovation: The 4th UK Alternative Finance Industry Report*, University of Cambridge Judge Business School Centre for Alternative Finance (Dec. 2017), available at: *https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-12-21-ccaf-entrenching-innov.pdf* (U.K. market).

531. See, e.g., Secretary Wilbur Ross, *E.U. Data Privacy Laws are Likely to Create Barriers to Trade*, Financial Times (May 30, 2018).

include Hong Kong's Personal Data Ordinance on Privacy in 2012,[532] Australia's Consumer Data Right,[533] and Singapore's Personal Data Protection Act.[534]

Business Models

Nonbanks and technology-focused companies have played active roles in developing payments and credit-scoring systems to improve the access to and functionality of financial services, and to reduce costs. While access to payment clearing and settlement services is generally limited to depositary institutions in the United States, some countries have provided mechanisms that allow nonbanks to access those services. Notable examples include China and regions of Africa, where the payments market is heavily reliant on nonbank-operated chat or mobile phone text message systems.

In China, authorities have allowed nonbank fintechs to access payment systems to clear and settle retail payment transactions. Large nonbank firms, like Ant Financial (AliPay) and Tencent (WeChat) have established dominant positions in the Chinese mobile payments market, with 54.3% and 38.2% shares of the market, respectively, in 2017.[535] The mobile wallets and payments mechanisms allow consumers to make payments while shopping online or through a messaging app, and provide access to other financial services offered within the ecosystem of the company that owns the mobile wallet.[536]

M-PESA, which began in Kenya, is another example of a nonbank payments company that operates outside a bank-centric payments ecosystem. It is operated by a telecommunications company and allows customers to make and receive payments using a mobile phone, without the need for a bank account. As of year-end 2016, M-PESA was live in 10 countries, had 29.5 million active customers, and processed about 6 billion transactions.[537]

Given the success of these nonbank models in some jurisdictions, it is not surprising that many analysts are estimating that a significant share of financial institutions' volumes and profits around

---

532. Privacy Commissioner for Personal Data (Hong Kong), *The Ordinance at a Glance*, available at: *https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html* (last accessed June 29, 2018).

533. As announced on November 26, 2017, the Consumer Data Right (CDR) is intended as an economy-wide right, to be applied sector-by-sector on the designation of the Australian Treasurer. The Treasurer will be leading the development of the CDR, with the design of the broader CDR informed by the government's response to the recommendations of its open banking review. See The Treasury (Australia), *Consumer Data Right – Fact Sheet*, available at: *http://static.treasury.gov.au/uploads/sites/1/2018/02/180208-CDR-Fact-Sheet-1.pdf* (last accessed June 29, 2018).

534. Personal Data Protection Commission (Singapore), *Legislation and Guidelines Overview*, available at: *https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview* (last accessed June 29, 2018).

535. Don Weinland, *Tencent Closes in on Alipay Crown*, Financial Times (Apr. 3, 2018).

536. Mancy Sun et al., Goldman Sachs Equity Research, *The Rise of China Fintech* (Aug. 7, 2017); Wei Wang and David Dollar, Brookings Institution, *What's Happening with China's FinTech Industry* (Feb. 2018), available at: *https://www.brookings.edu/blog/order-from-chaos/2018/02/08/whats-happening-with-chinas-fintech-industry/*.

537. Vodafone Group Plc., *Press Release – Vodafone Marks 10 Years of the World's Leading Mobile Money Service, M-Pesa* (Feb. 21, 2017), available at: *http://www.vodafone.com/content/index/media/vodafone-group-releases/2017/m-pesa-10.html#*.

the world are at risk of disruption from technology-driven business models.[538] In particular, technology firms are expected to take advantage of new open-banking paradigms, such as Europe's PSD2 or India's UPI, for instance, by using messaging platforms to access the country's real-time payment system.

New Technologies

In this changing international landscape, the intersection of technological advancement, data privacy, and industrial policy has put pressure on globally active firms. As they confront technological innovation, some foreign governments have attempted to restrict access to U.S. firms by, for example, requiring data to be stored and processed locally, putting caps on foreign ownership, forcing joint ventures, and enforcing discriminatory licensing requirements. These restrictions have a range of commercial consequences for those firms and may conflict with regulatory objectives, both in the United States and abroad.

Interest in crypto-assets from a range of financial authorities has increased substantially over the past year, as evidenced in the March 2018 G20 Finance Ministers and Central Bank Governors Communiqué. For the first time, the G20 explicitly addressed crypto-assets, and assigned the Financial Stability Board (FSB) "in consultation with other standard-setting bodies, including the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions, and Financial Action Task Force (FATF) to report in July 2018 on their work on crypto-assets." The resulting report sets out the metrics that the FSB will use to monitor crypto-asset markets as part of its ongoing assessment of vulnerabilities in the financial system.[539] The G20 authorities are cognizant of the inherent risks these new assets currently pose for investor protection and anti-money laundering and illicit finance regimes.

March 2018 G20 Communiqué

We acknowledge that technological innovation, including that underlying crypto-assets, has the potential to improve the efficiency and inclusiveness of the financial system and the economy more broadly. Crypto-assets do, however, raise issues with respect to consumer and investor protection, market integrity, tax evasion, money laundering and terrorist financing. Crypto-assets lack the key attributes of sovereign currencies. At some point they could have financial stability implications. We commit to implement the FATF standards as they apply to crypto-assets, look forward to the FATF review of those standards, and call on the FATF to advance global implementation. We call on international standard-setting bodies to continue their monitoring of crypto-assets and their risks, according to their mandates, and assess multilateral responses as needed.

Source: Communique of the G20 Finance Minsters & Central Bank Governors, Buenos Aires, Argentina (March 19-20, 2018).

538. Miklós Dietz et al., McKinsey & Company, *Remaking the Bank for an Ecosystem World* (Oct. 2017), available at: *https://www.mckinsey.com/industries/financial-services/our-insights/remaking-the-bank-for-an-ecosystem-world* (estimating that 65% of bank profits are under threat from nonbank players, like large technology platform companies); Aaron Fine and Rick Chavez, Oliver Wyman, *The Customer Value Gap: Re-Calculating the Route* (2018), available at: *http://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/January/state-of-the-financial-industry-2018-web.pdf*.

539. Financial Stability Board, *Crypto-Assets: Report to the G20 on Work by the FSB and Standard-Setting Bodies* (July 16, 2018), available at: *http://www.fsb.org/wp-content/uploads/P160718-1.pdf*.

Related to these issues, but separate from the focus on crypto-assets, is continuing international interest in the underlying technology. The financial services industry is already developing applications for distributed ledger technology (DLT), including in commodities trading and securities settlement, property registries, and secure, trusted identity products and services, among other use-cases. Some central banks have contemplated the potential for central bank-backed digital currencies, or a tokenized form of a fiat currency that utilizes DLT, asserting that they could potentially help reduce fees, processing times, and operational risk for market participants. Whether such potential benefits could materialize is still highly uncertain. Some central bankers are also considering how to use DLT to conduct interbank payments or employ DLT as a basis for other financial infrastructure, including through Project Ubin at the Monetary Authority of Singapore and Project Jasper at the Bank of Canada. Private consortiums are also experimenting with permissioned distributed ledgers, which operate by allowing only a known set of participants to validate transactions.

International Engagement

The United States engages with international counterparts on a bilateral and multilateral basis to advance U.S. interests abroad. Given the cross-border implications of financial technology, international bodies have established various groups focused on financial innovation. Financial authorities from the United States participate in international forums such as G20, the FSB, and International Monetary Fund to identify and manage global challenges, mitigate financial stability risks, and strengthen the external environment for U.S. growth. Additionally, U.S. authorities monitor developments and gather information to inform U.S. regulatory and supervisory approaches and priorities.

The United States strives to advance a coordinated policy approach at relevant international forums and standard-setting bodies. As financial technologies evolve, the emerging regulatory issues stemming from financial innovation often mean that U.S. authorities are in the process of developing a domestic regulatory approach at the same time that international organizations and standard-setting bodies are determining an international agenda. It is important that the United States remain engaged in these international discussions to ensure that any outcomes are consistent with domestic priorities.

International organizations have ramped up work on financial innovation in response to members' demand. However, U.S. authorities should guard against international standards being prematurely adopted before domestic policy is sufficiently advanced. International forums offer important opportunities for U.S. regulatory authorities to share experiences and gather information about the implications of financial innovation for policy objectives such as financial stability, investor protection, and illicit finance regimes. Financial innovations can pose fresh questions and challenges for regulatory authorities, and there is a tension between taking time to develop competency and experience relevant to a new technology and adopting a regulatory framework for that technology in a timely manner. For this reason, international regulatory approaches and standards should be developed in coordination with market participants to ensure the regulatory regime is appropriately calibrated.

Given the nature of innovations in financial technology, cybersecurity is of critical importance, and the United States remains committed to building cyber resilience in the financial sector domestically

and internationally. Internationally, the United States is engaging with foreign counterparts on cybersecurity in the financial sector through several key multilateral and bilateral partnerships. At the G-7, Treasury co-chairs the Cybersecurity Expert Group (CEG) with the Bank of England. The CEG discusses approaches to financial sector cybersecurity, with the objective of fostering common understandings and collaboration on areas of interest. The G-7, through the CEG, continues to work toward building cyber resilience internationally in the financial services sector.

Figure 25 illustrates the various initiatives related to financial innovation underway in a number of prominent international bodies. Treasury continues to engage closely with other U.S. agencies, including those representing the United States at the Committee on Payments and Market Infrastructures, the International Organization of Securities Commissions, FATF, and other international bodies, to maintain a unified message — namely that we support responsible innovation in the marketplace, while maintaining the integrity and accessibility of the financial system. It is important that we stay vigilant to the international discussions on financial innovation, particularly any which may result in the potential development of standards or best practices, to ensure that any outcomes are balanced and consistent with the U.S. approach.

Recommendations

Treasury should continue to leverage international bodies to support our domestic agenda, with domestic financial and regulatory priorities guiding the positions we take in international forums. Treasury will work to ensure actions taken by international organizations align with U.S. national interests and the domestic priorities of U.S. regulatory authorities. Treasury believes in avoiding regulatory fragmentation where possible, and promoting international approaches that facilitate cross-border capital and investment flows. It would be premature, however, to develop international regulatory standards for many applications of financial technology currently under discussion. In these cases, Treasury recommends continued participation by relevant experts in international forums and standard-setting bodies to share experiences regarding respective regulatory approaches and to benefit from lessons learned. Market participants require regulatory clarity to operate, but that clarity must start from domestic authorities determining the right approach within their own jurisdictions.

Treasury and U.S. financial regulators should engage with the private sector with respect to ongoing work programs at international bodies to ensure regulatory approaches are appropriately calibrated. Discussions on financial innovation occurring in international organizations sometimes do not include relevant experts. Additionally, central banks, ministries of finance, and capital markets regulators must continue building relevant in-house expertise regarding financial innovations such as cloud services, APIs, and artificial intelligence.

Finally, Treasury and U.S. financial regulators should proactively engage with international organizations to ensure that they are adhering to their core mandates. Standard-setting bodies should closely align their work and recommendations with the core competencies of each institution, including when they are addressing issues related to applications of financial technology.

Figure 25: International Interagency Fintech Collaboration Efforts

Group Name		
Participating agencies	**Mission / Goals**	**Correlation to Fintech**
The Bank for International Settlements, Committee on Payments and Markets Infrastructure and Committee on the Global Financial System		
Federal Reserve (committee chair) and the Federal Reserve Bank of New York represent the United States. Other members include other central banks.	Identify and assess potential sources of stress in global financial markets, further the understanding of the structural underpinnings of financial markets, and promote improvements to the functioning and stability of these markets.	Fintech Payments and Lending. From 2014 to February 2017, the Committee on Payments and Markets Infrastructure has published papers on a variety of fintech payments topics including DLT in payments, virtual currencies, faster payments, and nonbanks in retail payments papers.
Basel Committee on Banking Supervision's Task Force on Financial Technology (TFFT)		
OCC co-chairs, and FDIC and Federal Reserve also represent the United States. Other participants include central banks and authorities with formal responsibility for the supervision of banking business.	TFFT assesses the risks and supervisory challenges associated with innovation and technological changes affecting banking.	General Fintech. TFFT's work is currently focused on the effect that fintech has on banks and banks' business models, and the implications this has for supervision.
Financial Action Task Force (FATF) Fintech & Regtech Forums		
Treasury (lead), Federal Reserve and OCC represent the United States. Other members include agencies from other jurisdictions and two regional organizations, and associate members include other international and regional organizations.	Conduct industry outreach and provide a platform for a constructive dialogue and support innovation in financial services while addressing the regulatory and supervisory challenges posed by emerging technologies.	General Fintech. In 2017, FATF held three fintech-related events on fintech, regtech, and AML/countering the financing of terrorism (CFT) covering topics including: relevance of emerging fintech trends to financial institutions; AML/CFT standards in fintech; how different jurisdictions approach the regulation and supervision of fintech; fintech's effect on AML/CFT-related information availability and exchange; and risk management and mitigation for fintech.

Group Name		
Participating agencies	**Mission / Goals**	**Correlation to Fintech**
Financial Stability Board Financial Innovation Network		
Treasury, FRB, SEC, OCC, FDIC, FRBNY, and the Office of Financial Research represent the United States. Other members include central banks and authorities with formal responsibility for the supervision of banking business.	The Financial Stability Board promotes international financial stability by coordinating national financial authorities and international standard-setting bodies as they work toward developing financial sector policies. The Financial Innovation Network is responsible for understanding emerging trends in financial services and the potential effect on financial stability.	General Fintech. In 2017, published white papers and a report on the financial stability implications of fintech credit (in collaboration with the Committee on the Global Financial System), the use of artificial intelligence (AI) and machine learning in financial services, and fintech supervisory and regulatory issues that merit authorities' attention.
International Credit Union Regulators Network (ICURN)		
NCUA represents the United States. Other members include national and other supervisors of credit unions and financial cooperatives.	ICURN provides training to supervisors of credit unions and financial cooperatives on a variety of topics.	General Fintech. ICURN's July 2017 conference included a panel on understanding fintech and regulation. Discussion covered sectors including payments, lending, digital wealth management, and DLT.
International Organization of Securities Commissions (IOSCO), Committee on Emerging Risks		
SEC and CFTC represent the United States. Other members include national and provincial securities regulators.	IOSCO brings together the world's securities regulators and works with the G20 and the Financial Stability Board (FSB) on the global regulatory reform agenda. The Committee on Emerging Risks provides a platform for securities regulators and economists to discuss emerging risks and market developments and to develop and assess tools to assist regulators in reviewing the regulatory environment and identifying, monitoring, and managing systemic risk.	General Fintech. In February 2017, the Committee on Emerging Risks published a research report on fintech, which included sections on fintech lending, digital investment advice, DLT, fintech in emerging markets, and other regulatory considerations. IOSCO also established an Initial Coin Offering Consultation Network, through which members can discuss their experiences and concerns regarding token sales, and has issued related statements to members and the public.

Source: U.S. Government Accountability Office, *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight* (March 2018).

Appendix A

Participants in the Executive Order Engagement Process

Participants in the Executive Order Engagement Process

GOVERNMENT AND INTERNATIONAL

U.S. Federal and State

Appraisal Subcommittee of the Federal Financial Institutions Examination Council	Financial Crimes Enforcement Network
Arizona Attorney General's Office	Financial Industry Regulatory Authority
Board of Governors of the Federal Reserve System	Government National Mortgage Association (Ginnie Mae)
Bureau of Consumer Financial Protection	National Association of Consumer Credit Administrators
Bureau of the Fiscal Service – U.S. Department of the Treasury	National Credit Union Administration
Conference of State Bank Supervisors	North American Securities Administrators Association
Defense Innovation Unit Experimental (DIUx)	Office of the Comptroller of the Currency
Federal Communications Commission	U.S. Department of Homeland Security
Federal Deposit Insurance Corporation	U.S. Department of Housing and Urban Development
Federal Housing Administration	U.S. Commodity Futures Trading Commission
Federal Housing Finance Agency	U.S. Securities and Exchange Commission
Federal Trade Commission	

Non-United States

Bank of Canada	International Monetary Fund
Dutch National Bank	Monetary Authority of Singapore
European Commission	U.K. Financial Conduct Authority

EXPERTS AND ADVOCATES

Americans for Financial Reform	Mercatus Center at George Mason University
Autonomous NEXT	National Community Reinvestment Coalition
Bandman Advisors	National Consumer Law Center
CB Insights	Paul Hastings LLP
Center for Financial Services Innovation	Thomas W. Miller Jr., Mississippi State University College of Business
Center for Responsible Lending	U.S. Public Interest Research Group
David Yermack, New York University Stern School of Business	Urban Institute
Davis Polk & Wardwell LLP	Willkie Farr & Gallagher LLP
Delta Strategy Group	World Economic Forum
Marco Santori, Blockchain.com	
Michael Kitces, CFP	

TRADE ASSOCIATIONS

American Bankers Association	American Institute of Certified Public Accountants
American Financial Services Association	American Land Title Association

American Transaction Processors Coalition

CFA Institute

Community Financial Services Association of America

Consumer Bankers Association

Consumer Financial Data Rights

Electronic Transactions Association

Financial Innovation Now

Financial Planning Association

Financial Services Centers of America

Financial Services Information Sharing and Analysis Center

Financial Services Roundtable

Futures Industry Association

Global Financial Markets Association

Independent Community Bankers of America

International Swaps and Derivatives Association

Investment Adviser Association

Investment Company Institute

MarketPlace Lending Association

Money Service Business Association

Mortgage Bankers Association

National Association of Auto Dealers

National Association of Personal Financial Advisors

National Association of Realtors

National Money Transmitters Association

Network Branded Prepaid Card Association

Online Lenders Alliance

Real Estate Valuation Advocacy Association

Receivables Management Association

Securities Industry and Financial Markets Association

Small Business Finance Association

Structured Finance Industry Group

The Appraisal Foundation

The Data Coalition

U.S. Chamber of Commerce

FIRMS	
Ace Cash Express	BNP Paribas
Advance America	Capital One
Affirm	Charles Schwab & Co.
Ally	Chase Mortgage Servicing
Amazon	Citigroup
American Education Services/ PHEAA	CLS Bank
American Express	Coinbase
American Honda Finance Corporation	CommonBond
Andreesen Horowitz	Compass Point Research and Trading
Apple Pay	ConsenSys
Avant	CoreLogic
Bank of America	Credit Karma
Bayview Loan Servicing	Credit Suisse
BBVA	Cross River Bank
Better Mortgage	Depository Trust and Clearing Corporation
Betterment	DRW Venture Capital
Black Knight, Inc.	DV01
BlackRock/FutureAdvisor	E*TRADE
Blend	Early Warning
Blooom	Ellie Mae
Bloq	Encore Capital

Envestnet | Yodlee

Experian North America

Facebook

Fair Isaac Corporation (FICO)

Fannie Mae

Fay Servicing

Fidelity Investments

Financial Engines

First Data

FIS

Folio Investing

Freddie Mac

FT Partners

Funding Circle

Goldman Sachs

Google

Great Lakes

Intercontinental Exchange

Intercontinental Exchange/ MERSCORP

Intuit

Invesco

JPMorgan Chase

Kabbage

Keefe, Bruyette & Woods

Lightspeed Venture Partners

LeadsMarket

LedgerX

Legal & General Investment Management America

Lend360

Lending Club

LoanCare

LoanDepot

Mastercard

Microsoft Azure

Mid America Mortgage

MOHELA

MoneyGram

Moneytree

Moody's

Morgan Stanley

Morningstar

Mortgage Investors Group

Mr. Cooper

NASDAQ

Navient

Nelnet

NextCapital Group

NOIC/Concord

Ocwen Financial

One Main Financial

Orchard Platform

PayPal

PeerIQ

PennyMac Financial Services

Plaid

PNC Financial

Primary Residential Mortgage

Prosper

Quicken Loans

R3

Ripple

S&P Global

Select Portfolio Servicing

Sequoia Capital

Silicon Valley Bank

SoFi

Square

Stripe

T. Rowe Price

TD Ameritrade

The Clearing House Payments Company

Toyota Financial Services

TransUnion

Tricadia Capital

TSYS

Two Sigma Investments

U.S. Bancorp

United Income

Upstart

Vanguard

Veritec Solutions

Veros

Viamericas

Visa

Wealthfront

WebBank

Wells Fargo Mortgage Servicing

Western Asset Management

Western Union

WorldPay (Vantiv)

ZestFinance

Appendix B

Table of Recommendations

Table of Recommendations

Embracing Digitization, Data, and Technology

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Digitization			
Telephone Consumer Protection Act (TCPA) and Fair Debt Collection Practices Act (FDCPA)			
Treasury recommends that the FCC continue its efforts to address the issue of unwanted calls through the creation of a reassigned numbers database. Treasury recommends that the FCC create a safe harbor for calls to reassigned numbers that provides callers a sufficient opportunity to learn the number has been reassigned.		FCC	F, G
Treasury recommends that the FCC provide clear guidance on reasonable methods for consumers to revoke consent under the TCPA. Congress should consider statutory changes to the TCPA to mitigate unwanted calls to consumers and provide for a revocation standard similar to that provided under the FDCPA.	Congress	FCC	A, F
Treasury recommends that the Bureau promulgate regulations under the FDCPA to codify that reasonable digital communications, especially when they reflect a consumer's preferred method, are appropriate for use in debt collection.		Bureau	A, F
Consumer Financial Data			
Consumer Access to Financial Account and Transaction Data			
Treasury recommends that the Bureau affirm that for purposes of Section 1033, third parties properly authorized by consumers, including data aggregators and consumer fintech application providers, fall within the definition of "consumer" under Section 1002(4) of Dodd-Frank for the purpose of obtaining access to financial account and transaction data.		Bureau	A, F
Treasury recommends that regulators such as the SEC, Financial Industry Regulatory Authority, DOL, and state insurance regulators recognize the benefits of consumer access to financial account and transaction data in electronic form and consider what measures, if any, may be needed to facilitate such access for entities under their jurisdiction. However, Treasury recommends against further legislative action to expand the scope of Section 1033 at this time.	Congress	SEC, FINRA, DOL, State Insurance Regulators	A
Treasury recommends that the Bureau work with the private sector to develop best practices on disclosures and terms and conditions regarding consumers' use of products and services powered by consumer financial account and transaction data provided by data aggregators and financial services companies. If necessary, the Bureau should consider issuing principles-based disclosure rules pursuant to its authority under Section 1032 of Dodd-Frank.		Bureau	A, F

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury believes that consumers should have the ability to revoke their prior authorization that permits data aggregators and fintech applications to access their financial account and transaction data. Data aggregators and fintech applications should provide adequate means for consumers to readily revoke the prior authorization. If necessary, banking regulators and the SEC should consider issuing rules that require financial services companies to comply with a consumer request to limit, suspend, or terminate access to the consumer's financial account and transaction data by data aggregators and fintech applications.		FRB, FDIC, OCC, SEC	A, F
Treasury sees a need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data sharing agreements that effectively move firms away from screen-scraping to more secure and efficient methods of data access. Treasury believes that the U.S. market would be best served by a solution developed by the private sector, with appropriate involvement of federal and state financial regulators. A potential solution should address data sharing, security, and liability. Any solution should explore efforts to mitigate implementation costs for community banks and smaller financial services companies with more limited resources to invest in technology.		FRB, FDIC, OCC, SEC, FINRA, State Regulators	A
Treasury recommends that any potential solution discussed in the prior recommendation also address resolution of liability for data access. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.	Congress	FRB, FDIC, OCC, SEC, FINRA, State Regulators	A, F
Treasury recommends that any potential solution discussed in the prior recommendation address the standardization of data elements as part of improving consumers' access to their data. Any solution should draw upon existing efforts that have made progress on this issue to date. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.	Congress	FRB, FDIC, OCC, SEC, FINRA, State Regulators	A, F

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury recommends that the banking regulators remove ambiguity stemming from the third-party guidance that discourages banks from moving to more secure methods of data access such as APIs.		FRB, FDIC, OCC, Bureau	A, F
To the extent that any additional regulation of data aggregation is necessary, Treasury recommends that it occur at the federal level by regulators that have significant experience in data security and privacy, and that will have, through legislation if necessary, broad jurisdiction to ensure equivalent treatment in the nonfinancial sector.	Congress		F, G
Data Security and Breach Notification			
Treasury recommends that Congress enact a federal data security and breach notification law to protect consumer financial data and notify consumers of a breach in a timely manner. Such a law should be based on the following principles: protect consumer financial data; ensure technology-neutral and scalable standards based on the size of an entity and type of activity in which the entity engages; recognize existing federal data security requirements for financial institutions; and employ uniform national standards that preempt state laws.	Congress		F, G
Digital Legal Identity			
Treasury recommends that financial regulators work with Treasury to enhance public-private partnerships to identify ways government can eliminate unintended or unnecessary regulatory and other barriers and facilitate the adoption of trustworthy digital legal identity products and services in the financial services sector. Treasury also recognizes that the development of digital legal identity products and services in the financial services sector should be implemented in a manner that is compatible with solutions developed across other sectors of the U.S. economy and government.		Treasury, FinCEN, FRB, FDIC, OCC, SEC, State Regulators	F
Treasury supports the efforts of OMB to fully implement the long-delayed U.S. government federated digital identity system. Treasury recommends policies that would restore a public-private partnership model to create an interoperable digital identity infrastructure and identity solutions that comply with NIST guidelines and would reinvigorate the role of U.S. government-certified private sector identity providers, promoting consumer choice and supporting a competitive digital identity marketplace.		OMB, GSA, Commerce	F

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
The Potential of Scale			
Cloud Technologies and Financial Services			
Treasury recommends that federal financial regulators modernize their requirements and guidance (e.g., vendor oversight) to better provide for appropriate adoption of new technologies such as cloud computing, with the aim of reducing unnecessary barriers to the prudent and informed migration of activities to the cloud. Specific actions U.S. regulators should take include: formally recognizing independent U.S. audit and security standards that sufficiently meet regulatory expectations; addressing outdated record keeping rules like SEC Rule 17a-4; clarifying how audit requirements may be met; setting clear and appropriately tailored chain outsourcing expectations; and providing staff examiners appropriate training to implement agency policy on cloud services.		FRB, FDIC, OCC, SEC, CFTC, SROs	D, F
Treasury recommends that a cloud and financial services working group be established among financial regulators so that cloud policies can benefit from deep and sustained understanding by regulatory authorities. Financial regulators should support potential policies by engaging key industry stakeholders, including providers, users, and others impacted by cloud services. U.S. financial regulators should seek to promote the use of cloud technology within the existing U.S. regulatory framework to help financial services companies reduce the risks of noncompliance as well as the costs associated with meeting multiple and sometimes conflicting regulations. Regulators should be wary of imposing data localization requirements and should instead seek other supervisory or appropriate technological solutions to potential data security, privacy, availability, and access issues.		Treasury, FRB, FDIC, OCC, SEC, CFTC, SROs	D, F
Big Data, Machine Learning, and Artificial Intelligence in Financial Services			
Regulators should not impose unnecessary burdens or obstacles to the use of AI and machine learning and should provide greater regulatory clarity that would enable further testing and responsible deployment of these technologies by regulated financial services companies as the technologies develop.		Federal and State Financial Regulators	D, F
Treasury recommends that financial regulators engage with the Select Committee on Artificial Intelligence, in addition to pursuing other strategic interagency AI efforts. Engagement in such efforts should emphasize use-cases and applications in the financial services industry, including removing regulatory barriers to deployment of AI-powered technologies.		Federal Financial Regulators	D, F

Aligning the Regulatory Framework to Promote Innovation

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Modernizing Regulatory Frameworks for National Activities			
Improving the Clarity and Efficiency of Our Regulatory Frameworks			
Treasury supports state regulators' efforts to build a more unified licensing regime and supervisory process across the states. Such efforts might include adoption of a passporting regime for licensure. However, critical to this effort are much more accelerated actions by state legislatures and regulators to effectively reduce unnecessary inconsistencies across state laws and regulations to achieve much greater levels of harmonization. Treasury recommends that if states are unable to achieve meaningful harmonization across their licensing and supervisory regimes within three years, Congress should act to encourage greater uniformity in rules governing lending and money transmission to be adopted, supervised, and enforced by state regulators.	Congress	State Regulators	A, D, F
Treasury recommends that the OCC move forward with prudent and carefully considered applications for special purpose national bank charters. OCC special purpose national banks should not be permitted to accept FDIC-insured deposits, to reduce risks to taxpayers. The OCC should consider whether it is appropriate to apply financial inclusion requirements to special purpose national banks. The Federal Reserve should assess whether OCC special purpose national banks should receive access to federal payment services.		FRB, OCC	A, B, D, F

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Federal banking regulators should, in coordination, review current third-party guidance through a notice and comment process. U.S. banking regulators should further harmonize their guidance with a greater emphasis on (1) improving the current tailoring and scope of application of guidance upon third-party vendors to improve the efficiency of oversight and (2) enabling innovations in a safe and prudent manner. Such a review should specifically consider how to: • Further develop the framework to regulate bank partnerships with fintech lenders to apply strong and tailored regulatory oversight while also supporting efforts by banks, particularly smaller community banks, to partner with fintechs. • Provide greater clarity around the vendor oversight requirements for cloud service providers, including clarifying how third-party guidance should apply to a third-party's sub-contractors, like cloud service providers (i.e., fourth party vendors). • Support more secure methods for consumers to access their financial data, such as through API agreements between banks and data aggregators. • Identify common tools banks can leverage as part of due diligence efforts, such as robust independent audits, recognized certifications, and collaboration among institutions in an effort to enhance efficiencies and reduce costs. • Maintain ongoing efforts with other federal and state regulators to identify opportunities for harmonization as appropriate. Looking ahead and recognizing the dynamic nature of financial technology developments, the banking regulators should be prepared to flexibly adapt their third-party risk relationships framework to emerging technology developments in financial services. Moreover, banking regulators should consider how to make examiners' application of interagency guidance on third-party relationships more consistent across and within the agencies.		FRB, FDIC, OCC	A, D, F, G
Treasury recommends that the Federal Reserve consider how to reassess the definition of BHC control to provide firms a simpler and more transparent standard to facilitate innovation-related investments. This recommendation is consistent with public comments by Federal Reserve officials who have called for reassessing this issue. In addition, the banking regulators should interpret banking organizations' permitted scope of activities in a harmonized manner as permitted by law wherever possible and in a manner that recognizes the positive impact that changes in technology and data can have in the delivery of financial services.		FRB, FDIC, OCC	A, D, F, G

Updating Activity-Specific Regulations

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Lending and Servicing			
Marketplace Lending			
Treasury recommends that Congress codify the "valid when made" doctrine to preserve the functioning of U.S. credit markets and the long-standing ability of banks and other financial institutions, including marketplace lenders, to buy and sell validly made loans without the risk of coming into conflict with state interest rate limits. Additionally, the federal banking regulators should use their available authorities to address challenges posed by *Madden*.	Congress	FRB, FDIC, OCC	A, F
Treasury recommends that Congress codify that the existence of a service or economic relationship between a bank and a third party (including financial technology companies) does not affect the role of the bank as the true lender of loans it makes. Further, federal banking regulators should also reaffirm (through additional clarification of applicable compliance and risk-management requirements, for example) that the bank remains the true lender under such partnership arrangements.	Congress	FRB, FDIC, OCC	A, F
Treasury recognizes the role of state laws and oversight in protecting consumers, but such state regulation should not occur in a manner that hinders bank partnership models already operating in a safe and sound manner with appropriate consumer protections. Treasury recommends that states revise credit services laws to exclude businesses that solicit, market, or originate loans on behalf of a federal depository institution pursuant to a partnership agreement.		States	A, F
Mortgage Lending and Servicing			
Treasury recommends that Ginnie Mae pursue acceptance of eNotes and supports the measures outlined in its *Ginnie Mae 2020* roadmap to more broadly develop its digital capabilities.		HUD / Ginnie Mae	A, F
Treasury recommends Congress appropriate for FHA the funding it has requested for technology upgrades in the President's Fiscal Year 2019 Budget – a portion of which FHA would use to improve the digitization of loan files. In addition, FHA, VA, and USDA should explore the development of shared technology platforms, including for certain origination and servicing activities.	Congress	HUD / FHA, VA / USDA	A, F
Treasury recommends the FHLBs explore ways to address their concerns regarding eNotes with the goal of accepting eNotes on collateral pledged to secure advances.		FHLBs	A, F
Treasury recommends that Congress revisit Title XI FIRREA appraisal requirements to update them for developments that have occurred in the market during the past thirty years. An updated appraisal statute should account for the development of automated and hybrid appraisal practices and sanction their use where the characteristics of the transaction and market conditions indicate it is prudent to do so.	Congress		A, F

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury recommends FHA and other government loan programs develop enhanced automated appraisal capabilities to improve origination quality and mitigate the credit risk of overvaluation. These programs may also wish to consider providing targeted appraisal waivers where a high degree of property standardization and information about credit risk exists to support automated valuation, and where the overall risks of the mortgage transaction make such a waiver appropriate. Treasury supports legislative action where statutory changes are required to authorize granting limited appraisal waivers for government programs.	Congress	HUD / FHA, VA, USDA	A, F
Treasury further recommends that government loan programs explore opportunities to leverage industry-leading technology capabilities to reduce costs to taxpayers and accelerate adoption of new technology in the government-insured sector.		HUD / FHA, VA, USDA	A, F
Treasury recommends that states yet to authorize electronic and remote online notarization pursue legislation to explicitly permit the application of this technology and the interstate recognition of remotely notarized documents. Treasury recommends states align laws and regulations to further standardize notarization practices.		States	A, F
Treasury recommends Congress consider legislation to provide a minimum uniform standard for electronic and remote online notarizations.	Congress		A, F
Treasury recommends that recording jurisdictions yet to recognize and accept electronic records implement the necessary technology updates to process and record these documents and to pursue digitization of existing property records.		States	A, F
To address the perception associated with the use of the FCA on mortgage loans insured by the federal government, Treasury recommends that HUD establish more transparent standards in determining which program requirements and violations it considers to be material to assist DOJ in determining which knowing defects to pursue. In doing so, Treasury recommends that: • FHA clarify the remedies and liabilities lenders and servicers face, which could include, where appropriate, remedies such as indemnification and/or premium adjustments. Remedies should be correlated to the Defect Taxonomy. • FHA should continue to review and refine its lender and loan certifications and its loan review system, including the Defect Taxonomy. Lenders that make errors deemed immaterial to loan approval should receive safe harbor from a denial of claim and forfeiture of premiums. Lenders should receive a similar safe harbor for material violations that are cured based on remedies prescribed by FHA absent patterns which indicate a systemic issue. • HUD, in determining the appropriate remedies for violations of its program requirements, should consider the systemic nature of the problem, involvement or knowledge of the lender's senior management, overall quality of the originations of a specific lender, and whether or to what extent the loan defect may have impacted the incidence or severity of the loan default.		HUD / FHA	F

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury recommends that DOJ ensure that materiality for purposes of the FCA is linked to the standards in place at the agency administering the program to which the claim has been filed, and that DOJ and HUD work together to clarify the process by which mutual agreement is reached on the resolution of claims. Where a relator pursues *qui tam* action against a lender for a nonmaterial error or omission, DOJ, in consultation with HUD and FHA, should exercise its statutory authority to seek dismissal.		DOJ, HUD	F
Treasury recommends Congress consider appropriate remedial legislation if the recommended administrative actions are unsuccessful at achieving the desired result of increasing lender and servicer participation in federal mortgage programs.	Congress		F
Treasury recommends that federally supported mortgage programs explore standardizing the most effective features of a successful loss mitigation program across the federal footprint. Such standardization should broadly align a loss mitigation approach that facilitates effective and efficient loan modifications when in the financial interest of the borrower and investor, promotes transparency, reduces costs, and mitigates the impact of defaults on housing valuations during downturns.		FHFA / GSEs, HUD / FHA, VA, USDA	F
Treasury recommends HUD continue to review FHA servicing practices with the intention to increase certainty and reduce needlessly costly and burdensome regulatory requirements, while fulfilling FHA's statutory obligation to the Mutual Mortgage Insurance Fund (MMIF). In particular, Treasury recommends that FHA consider administrative changes to how penalties are assessed across FHA's multi-part foreclosure timeline to allow for greater flexibility for servicers to miss intermediate deadlines while adhering to the broader resolution timeline, as well as to better align with federal loss mitigation requirements now in place through the Bureau.		HUD / FHA	A, F
Treasury recommends FHA explore changes to its property conveyance framework to reduce costs and increase efficiencies by addressing the frequent and costly delays associated with the current process. As an additional measure, Treasury recommends that FHA continue to make appropriate use of, and consider expanding, programs which reduce the need for foreclosed properties to be conveyed to HUD, such as Note Sales and FHA's Claim Without Conveyance of Title.		HUD / FHA	A, F
Treasury recommends that states pursue the establishment of a model foreclosure law, or make any modifications they deem appropriate to an existing law, and amend their foreclosure statutes based on that model law.		States	A, F
Treasury recommends federally supported housing programs, including those administered by FHA, USDA, and VA, and the GSEs, explore imposing guaranty fee and insurance fee surcharges to account for added costs in states where foreclosure timelines significantly exceed the national average.		FHFA / GSEs, HUD / FHA, VA, USDA	A, F

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury recommends that Ginnie Mae collaborate with FHFA, the GSEs, and the Conference of State Bank Supervisors to expand and align standard, detailed reporting requirements on nonbank counterparty financial health, including terms and covenants associated with funding structures, to provide confidence that taxpayers are protected during a period of severe market stress.		HUD / Ginnie Mae, FHFA / GSEs, CSBS	B
Treasury supports Ginnie Mae's consideration of enhancing its counterparty risk mitigation approach, including through the imposition of stress testing requirements that can provide information on the financial health of servicer counterparties across an economic cycle.		HUD / Ginnie Mae	B
Treasury recommends Ginnie Mae have sufficient flexibility to charge guaranty fees appropriate to cover additional risk arising from changes in the overall market or at the program level.	Congress		B
Treasury recommends a comprehensive assessment of Ginnie Mae's current staffing and contracting policies, including the costs and benefits of alternative pay and/or contracting structures. Ginnie Mae would be better equipped to manage its program and monitor counterparty risk if it were able to more readily attract personnel with requisite expertise by paying salaries comparable to those at other financial agencies with premium pay authority. Additionally, being able to adopt similar contracting procedures as other agencies that are outside of federal acquisition statutes and regulations would enable Ginnie Mae to more effectively monitor and respond to changing market conditions and needs. However, any change to Ginnie Mae's personnel or contracting policies should be informed by a comprehensive assessment of current challenges. The potential benefits of alternative pay and/or contracting structures should be weighed against the additional federal costs that would be incurred.	Congress	HUD / Ginnie Mae	B
Student Lenders and Servicers			
Education should establish guidance on minimum standards specifying how servicers should handle decisions with significant financial implications (e.g., payment application across loans, prioritizing repayment plans, and use of deferment and forbearance options), minimum contact requirements, standard monthly statements, and timeframes for completing certain activities (e.g., processing forms or correcting specific account issues). Treasury applauds the required use of Education branding on servicing materials in the new Direct Loan servicing procurement to reduce borrower confusion.		ED	F
In Education's new Direct Loan Servicing contract, Education should require student loan servicers to make greater use of emails and provide guidance to servicers on how to use email appropriately to balance privacy and security concerns with the need for effective and timely communication. All emails sent to federal student loan borrowers should provide enough information for borrowers to easily discern whether action must be taken on their account.		ED	A, F

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Education should contract with providers of secure e-signature software and cloud technology for use by federal student loan servicers on all forms.		ED	F
Education's Office of Federal Student Aid should include in its management team individuals with significant expertise in managing large consumer loan portfolios.		ED	B, F
Education should take steps to address existing data quality issues to better monitor and manage portfolio performance. Education should increase transparency by publishing greater portfolio performance data, servicer performance data, and cost estimation analysis on its website to give stakeholders greater insight into Education's management of the taxpayer investment in higher education.		ED	B, F
Treasury supports legislative efforts to implement a risk-sharing program for institutions participating in the federal student loan program based on the amount of principal repaid following five years of payments. Schools whose students have systematically low loan repayment rates should be required to repay small amounts of federal dollars in order to protect taxpayers' growing investment in the federal student loan program. Congress should consider how to address schools with systematically low repayment rates but large populations of disadvantaged students.	Congress	ED	F
Short-Term, Small-Dollar Installment Lending			
Treasury recognizes and supports the broad authority of states that have established comprehensive product restrictions and licensing requirements on nonbank short-term, small-dollar installment lenders and their products. As a result, Treasury believes additional federal regulation is unnecessary and recommends the Bureau rescind its Payday Rule.		Bureau	F, G
Treasury recommends the federal and state financial regulators take steps to encourage sustainable and responsible short-term, small-dollar installment lending by banks. Specifically, Treasury recommends that the FDIC reconsider its guidance on direct deposit advance services and issue new guidance similar to the OCC's core lending principles for short-term, small-dollar installment lending.		FRB, FDIC, OCC, Bureau, State Financial Regulators	A, D, F
Debt Collection			
Treasury recommends the Bureau establish minimum effective federal standards governing the collection of debt by third-party debt collectors. Specifically, these standards should address the information that is transferred with a debt for purposes of debt collection or in a sale of the debt. Further, the Bureau should determine whether the existing FDCPA standards for validation letters to consumers should be expanded to help the consumer assess whether the debt is owed and determine an appropriate response to collection attempts. Treasury does not support broad expansion of the FDCPA to first-party debt collectors absent further Congressional consideration of such action.		Bureau	F, G

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
IRS Income Verification			
It is important that IRS update its income verification system to leverage a modern, technology-driven interface that protects taxpayer information and enables automated and secure data sharing with lenders or designated third parties. Treasury recommends Congress fund IRS modernization, which would include upgrades that will support more efficient income verification.	Congress	Treasury	D, F, G
New Credit Models and Data			
Treasury recognizes that these new credit models and data sources have the potential to meaningfully expand access to credit and the quality of financial services. Treasury, therefore, recommends that federal and state financial regulators further enable the testing of these newer credit models and data sources by both banks and nonbank financial companies.		Federal and State Financial Regulators	A, D
Regulators, through interagency coordination wherever possible, should tailor regulation and guidance to enable the increased use of these models and data sources by reducing uncertainties. In particular, regulators should provide regulatory clarity for the use of new data and modeling approaches that are generally recognized as providing predictive value consistent with applicable law for use in credit decisions.		Federal and State Financial Regulators	D, F, G
Regulators should in general be willing to recognize and value innovation in credit modelling approaches. Regulators should enable prudent experimentation with the aim of working through various issues raised, which may in turn require new approaches to supervision and oversight.		Federal and State Financial Regulators	D, F, G
Credit Bureaus			
The FTC should retain its rulemaking and enforcement authority for nonbank financial companies under the GLBA. Additionally, Treasury recommends that the relevant agencies use appropriate authorities to coordinate regulatory actions to protect consumer data held by credit reporting agencies and that Congress continue to assess whether further authority is needed in this area.	Congress	FTC, Bureau	F, G
Treasury recommends that Congress amend CROA to exclude the national credit bureaus and national credit scorers (i.e., credit scoring companies utilized by financial institutions when making credit decisions) from the definition of "credit repair organization" in CROA.	Congress		F, G
InsurTech			
Lawmakers, policymakers, and regulators should take coordinated steps to encourage the development of innovative insurance products and practices in the United States. Domestically, this includes consideration of improving product speed to market, creating increased regulatory flexibility, and harmonizing inconsistent laws and regulations.	Congress	Federal and State Financial Regulators	F, G

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury's Federal Insurance Office, which provides insurance expertise in the federal government, should work closely with state insurance regulators, the NAIC, and federal agencies on InsurTech issues.		Treasury, Insurance Regulators, NAIC	F, G
Payments			
Money Transmitters			
Treasury supports the Bureau's ongoing efforts to reassess Regulation E. Treasury recommends that the Bureau provide more flexibility regarding the issuance of Regulation E disclosures and raise the current 100 transfer per annum threshold for applicability of the de minimis exemption.		Bureau	A, C, F, G
Faster Payments			
Treasury recommends that the Federal Reserve set public goals and corresponding deadlines consistent with the overall conclusions of the Faster Payments Task Force's final report.		FRB	C, D, F
Treasury recommends that the Federal Reserve move quickly to facilitate a faster retail payments system, such as through the development of a real-time settlement service, that would also allow for more efficient and ubiquitous access to innovative payment capabilities. In particular, smaller financial institutions, like community banks and credit unions, should also have the ability to access the most-innovative technologies and payment services.		FRB	C, D
Secure Payments			
Treasury recommends that continued work in the area of payment security include an actionable plan for future work, and ensure that solutions, especially in security, do not include specific tech mandates.		FRB, Treasury, Federal Financial Regulators	D, F
Wealth Management and Digital Financial Planning			
Treasury believes that appropriate protection for clients of financial planners, digital and otherwise, can be achieved without imposing either a fragmented regulatory structure or creating new regulatory entities. Treasury recommends that an appropriate existing regulator of a financial planner, whether federal or state, be tasked as the primary regulator with oversight of that financial planner and other regulators should exercise regulatory and enforcement deference to the primary regulator. To the extent that the financial planner is providing investment advice, the relevant regulator will likely be the SEC or a state securities regulator.		SEC, FINRA, DOL, Bureau, FRB, OCC, FDIC, State Regulators	A, F, G

Enabling the Policy Environment

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Agile and Effective Regulation for a 21st Century Economy			
Regulatory Sandboxes			
Treasury recommends that federal and state financial regulators establish a unified solution that coordinates and expedites regulatory relief under applicable laws and regulations to permit meaningful experimentation for innovative products, services, and processes. Such efforts would form, in essence, a "regulatory sandbox" that can enhance and promote innovation. If financial regulators are unable to fulfill those objectives, however, Treasury recommends that Congress consider legislation to provide for a single process consistent with the principles detailed in the report, including preemption of state laws if necessary.	Congress	Federal and State Financial Regulators, SROs	D, F, G
Agile Regulation			
Treasury recommends that Congress enact legislation authorizing financial regulators to use other transaction authority for research and development and proof-of-concept technology projects. Regulators should use this authority to engage with the private sector to better understand new technologies and innovations and their implications for market participants, and to carry out their regulatory responsibilities more effectively and efficiently.	Congress	Federal Financial Regulators	D, F
Treasury encourages regulators to appropriately tailor regulations to ensure innovative technology companies providing tools to regulated financial services companies can continue to drive technological efficiencies and cost reductions. Treasury encourages regulators to seek out and explore innovative partnerships with financial services companies and regtech firms alike to better understand new technologies that have the potential to improve the execution of their own regulatory responsibilities more effectively and efficiently.		Federal and State Financial Regulators	D, F
Treasury recommends that financial regulators pursue robust engagement efforts with industry and establish clear points of contact for industry and consumer outreach. Treasury recommends that financial regulators increase their efforts to bridge the gap between regulators and start-ups, including efforts to engage in different parts of the country rather than requiring entities to come to Washington, D.C.		Federal and State Financial Regulators, SROs	D, F, G
Treasury recommends that financial regulators periodically review existing regulations as innovations occur and new technology is developed and determine whether such regulations fulfill their original purpose in the least costly manner.		Federal and State Financial Regulators, SROs	D, F, G

Recommendation	Policy Responsibility		Core Principle
	Congress	Regulator	
Treasury recommends that financial regulators engage at both the domestic and international levels, as financial technology in many cases is borderless. Treasury encourages international initiatives by financial regulators to increase their knowledge of fintech developments in other nations.		Federal Financial Regulators	D, E, F
Critical Infrastructure			
Treasury recommends that financial regulators thoroughly consider cybersecurity and other operational risks as new technologies are implemented, firms become increasingly interconnected, and consumer data are shared among a growing number of firms, including third parties.		Federal and State Financial Regulators, SROs	B, C, D, F
Treasury recommends that the FBIIC consider establishing a technology working group charged with better understanding the technologies that firms are increasingly relying upon, and staying well-informed regarding innovation taking place within the sector.		FBIIC	F, G
Treasury commits to leading a multiyear program with the financial services industry to identify, properly protect, and remediate vulnerabilities.		Treasury	F, G
International Approaches and Consideration			
International Engagement			
Treasury recommends continued participation by relevant experts in international forums and standard-setting bodies to share experiences regarding respective regulatory approaches and to benefit from lessons learned. Treasury will work to ensure actions taken by international organizations align with U.S. national interests and the domestic priorities of U.S. regulatory authorities.		Federal Financial Regulators, Treasury	D, E
Treasury and U.S. financial regulators should engage with the private sector with respect to ongoing work programs at international bodies to ensure regulatory approaches are appropriately calibrated.		Federal Financial Regulators, Treasury	D, E
Treasury and U.S. financial regulators should proactively engage with international organizations to ensure that they are adhering to their core mandates.		Federal Financial Regulators, Treasury	D, E

Appendix C

Additional Background

Additional Background

Payments

Credit Card Networks

There are four predominant credit card networks in the United States that function through two different business models. These networks and business models were started, built, and remain as private-sector solutions that continue to be largely governed by private agreements instead of government mandates. The first model, a decentralized "open-loop" model of networks (e.g., Visa and Mastercard), began as associations that were jointly owned by banking institutions, but today are public companies. In this model, banks control the relationships with customers by issuing credit cards to consumers and signing up merchants for acquirer relationships. In this sense, the network is essentially a clearinghouse that facilitates acceptance and transaction routing for a fee; the banks generally set terms with their individual and business customers through contract.

Open-loop networks maintain their own rulebooks and limit their membership to licensed and regulated financial institutions. For example, in the United States, a member is required to be a depository institution or a chartered limited purpose national bank; in Europe, a member is required to be either a depository institution or a Payment Service Provider licensed under the Payment Services Directive.[540] The difference in licensing and chartering of various types of financial firms between the United States and other jurisdictions is a factor in the breadth of direct access to payment networks. Other jurisdictions such as the United Kingdom and India allow for a specialty kind of payment firm to be licensed and regulated by the Financial Conduct Authority[541] or Reserve Bank of India,[542] respectively. Such a licensing regime creates a regulatory framework for nondepository institutions that sets eligibility requirements for potential card network access.[543] However, these are baseline institutional eligibility criteria, and membership is not guaranteed just because such criteria are met — the card networks also have additional requirements and standards that must be met, such as having an effective AML regime.

The second model is a more centralized "closed-loop" structure (e.g., American Express and Discover). These firms, which also maintain their own rulebooks, are bank holding companies that run the payment network and control customer relationships by issuing cards and contracting with

---

540. See Visa, *Visa Europe Membership* (2015), at 4, available at: *https://www.visaeurope.com/media/images/44959_visa_membership_access_a4_pdf-73-25878.pdf*.

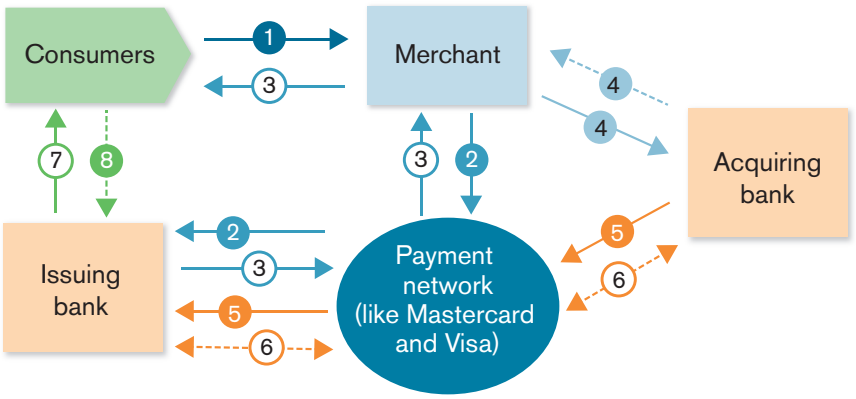
541. See Financial Conduct Authority, *Authorisation and Registration: E-money and Payment Institutions* (last updated Mar. 23, 2018), available at: *https://www.fca.org.uk/firms/authorisation-registration-emoney-payment-institutions*.

542. Reserve Bank of India, *Press Release–RBI Releases Guidelines for Licensing of Payments Banks* (Nov. 27, 2014), available at: *https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=32615*.

543. U.S. law allows the OCC to charter a special purpose credit card national bank, including a version that is exempt from requirements of the Bank Holding Company Act. This charter is only for banks whose predominant business is credit cards. See Office of the Comptroller of the Currency, *Comptroller's Licensing Manual: Charters* (Sept. 2016), at 51–54, available at: *https://www.occ.treas.gov/publications/publications-by-type/licensing-manuals/charters.pdf*. This charter is not common. As of March 31, 2018, only nine such bank charters were active. Office of the Comptroller of the Currency, *Credit Card Banks Active As of 3/31/2018*, available at: *https://www.occ.treas.gov/topics/licensing/national-banks-fed-savings-assoc-lists/credit-card-by-name-pdf.pdf*.

merchants themselves.[544] The open-loop networks authorize and clear the majority of credit card transactions. The open-loop, four-party credit card network model is illustrated below.

Figure C1: Credit Card Networks



1	The consumer pays a merchant with a credit card
2	The merchant then electronically transmits the data through the applicable Association's electronic network to the issuing bank for authorization
3	If approved, the merchant receives authorization to capture the transaction, and the cardholder accepts liability, usually by signing the sales slip
4	The merchant receives payment, net of fees, by submitting the captured credit card transactions to its bank (the acquiring bank) in batches or at the end of the day
5	The acquiring bank forwards the sales draft data to the applicable Association, which in turn forwards the data to the issuing bank. The Association determines each bank's net debit position. The Association's settlement financial institution coordinates issuing and acquiring settlement positions. Members with net debit positions (normally the issuing banks) send funds to the Association's settlement financial institution, which transmits owed funds to the receiving bank (generally the acquiring banks).
6	The settlement process takes place using a separate payment network such as Fedwire
7	The issuing bank presents the transaction on the cardholder's next billing statement
8	The cardholder pays the bank, either in full or via monthly payments

Source: Federal Deposit Insurance Corporation, *Risk Management Examination Manual for Credit Card Activities* (2007), at 165.

American Express and Discover, as bank holding companies, are subject to supervision and oversight by the Federal Reserve (and the banking regulator with jurisdiction over their banking subsidiaries) and the full suite of banking regulations. Visa and Mastercard are subject to regulation through the Bank Service Company Act as third-party service providers to banking organizations.

544. American Express and Discover now license their brands for issuance by other banking institutions in certain cases.

Debit Card Networks

Debit card networks are similar to credit card networks in that they are all private entities that maintain their own rules, regulations, and fee structures through private agreements and industry standards. Debit card networks are distinct in that they process a different type of transaction. Credit cards underlie a loan account with a bank — in authorizing the transaction, the card network is asking if the bank wants to approve addition to an open line of credit. Debit cards are attached to a pre-funded bank account — in authorizing the transaction, the card network is, in essence, asking the bank if sufficient funds are available for payment.[545]

There are two different types of debit networks in the United States: signature debit[546] and PIN debit.[547] Whereas all debit networks generally function as four-party systems (like the credit card networks) the infrastructure differs slightly between signature and PIN networks. Signature debit uses the credit card network infrastructure, and thus requires a "dual-message" — one message for authentication and one message for clearing. PIN debit, which evolved from ATM networks, uses a "single-message" authentication and clearing method whereby all the information is transmitted in one message.[548] This affects the speed of clearance and settlement between the two types of networks. Dual-message transactions are stored and then combined in a batch that is sent all at one time to the network providers. This is typically done once a day, but depending on merchant volume could be done more or less frequently. Single-message transactions have all the information necessary to clear the transaction at the time of authentication, with no need for batching or separate clearance. For both network types, there is only one settlement cutoff time, which is when funds are moved and interchange fees are determined. The speed at which this process is completed varies from same day for single-message, and upward of two days for dual-message.[549]

Signature debit networks generally charge higher interchange fees than PIN debit networks. According to the Federal Reserve, for all transactions for year-end 2016, the average interchange fees per transaction were for signature debit $0.33 (0.89% of average transaction value), and for PIN debit $0.24 (0.64% of average transaction value).[550] Signature debit networks are owned by the branded credit card networks whose logo is shown on the front of a debit card. PIN debit networks are owned both by credit card networks as well as merchant processors that provide back-end service; they are listed on the reverse side of a debit card.

---

545. This represents the basic structure of the transactions. Nuances may exist, for instance, banks may allow customers to overdraw, or let the balance go below zero on their bank accounts.

546. Signature debit networks: Visa, Mastercard, and Discover.

547. PIN debit networks (parent company): ACCEL (Fiserv), AFFN (FIS), ATH (Evertec), Credit Union 24 (Credit Union co-op), Interlink (Visa), Jeanie (Vantiv), Maestro (Mastercard), NetWorks, NYCE (FIS), PULSE (Discover), SHAZAM (member owned), STAR (First Data), and China UnionPay.

548. Debit Card Interchange Fees and Routing (June 30, 2011) [76 Fed. Reg. 43394, 43395 (July 20, 2011)].

549. Susan Herbst-Murphy, *Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts*, Federal Reserve Bank of Philadelphia Discussion Paper (2013), at 7-13, 22, available at: *https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2013/D-2013-October-Clearing-Settlement.pdf*.

550. Board of Governors of the Federal Reserve System, *Average Debit Card Interchange Fee by Payment Card Network* (last updated July 14, 2017), available at: *https://www.federalreserve.gov/paymentsystems/regii-average-interchange-fee.htm*.

Regulation of debit cards and credit cards is different. While both types of card transaction are regulated for consumer protection purposes, the rules derive from different statutes[551] and the implementing regulations[552] are codified separately. In some cases, these two regulations may have similar requirements that are implemented differently due to the nature of the product, such as consumer disclosures. Other requirements may be completely distinct, like the Durbin Amendment's application solely for debit cards.[553] And yet other requirements may be superseded by stricter contractual requirements imposed by the card networks, such as the card networks' requirement that all unauthorized card transactions carry zero liability for the cardholder.[554]

As for usage, debit cards see higher transaction volumes and values than credit cards. This disparity has been true for more than a decade and the popularity of debit cards in relation to credit cards continues to grow.

Figure C2: Total Number of Card Payments (billions) and Value ($ trillions)

	2015		2016	
	Number	Value	Number	Value
Total card payments	103.5	5.65	111.1	5.98
Debit cards	69.6	2.56	73.8	2.7
Non-prepaid	59	2.27	63	2.41
In person	49.5	1.58	52.1	1.66
Chip	0.4	0.02	8.4	0.37
No chip	49.1	1.56	43.7	1.29
Remote	9.5	0.69	10.9	0.75
Prepaid	10.6	0.3	10.7	0.29
General purpose	4.3	0.15	4.4	0.15
In person	3.6	0.1	3.6	0.1
Chip	0	0	0.1	0.01
No chip	3.6	0.1	3.5	0.1
Remote	0.8	0.05	0.8	0.05
Private label	3.6	0.07	3.8	0.07
Electronic benefits transfers (EBT)	2.6	0.08	2.5	0.07
Credit cards	33.9	3.08	37.3	3.27
General purpose	31	2.8	34.3	3
In person	21.7	1.3	23.4	1.36
Chip	1	0.08	6.6	0.47
No chip	20.7	1.22	16.8	0.89
Remote	9.3	1.5	10.9	1.64
Private label	2.8	0.28	3.1	0.27

Source: Federal Reserve System, *The Federal Reserve Payments Study - 2017 Annual Supplement.*

551. Credit cards: Truth in Lending Act, 15 U.S.C. § 1601 et seq.; Debit cards: Electronic Fund Transfer Act, 15 U.S.C. § 1693 et seq.

552. Credit cards: Regulation Z, 12 C.F.R. § 1026 et seq.; Debit cards: Regulation E, 12 C.F.R. § 1005 et seq.

553. 15 U.S.C. § 1693o-2.

554. See Visa, *Visa Core Rules and Visa Product and Service Rules*, Rule 1.4.6.1 (updated Oct. 2017), available at*: https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf*.

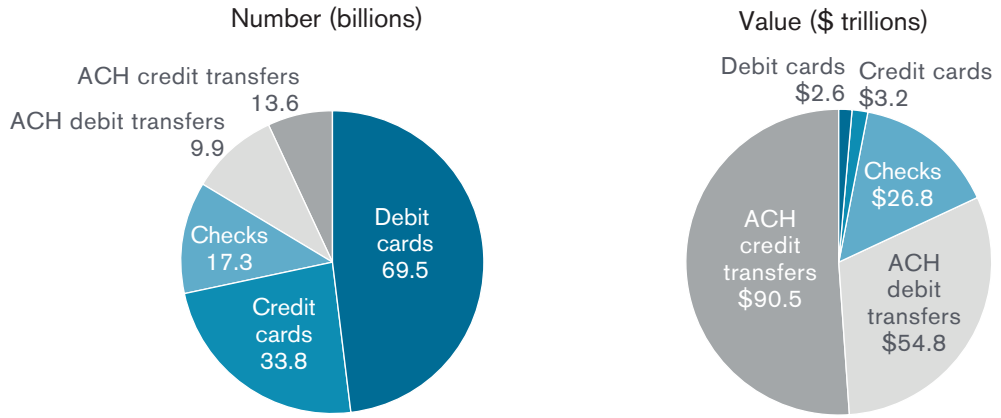
Access to card networks in the United States is largely set by private agreement and the system includes controls that ensure that each firm with direct access has a comprehensive and robust regulatory framework in place. Treasury believes that this system is working well and has supported innovative new solutions in the payments space. Treasury supports the private card networks' continual evaluation of their rulebooks in light of new entrants and innovations to the payments infrastructure to ensure that the systems continue to work well for all involved players.

Automated Clearing House (ACH)

The ACH network[555] is at the core of the payments system as one of the chief payment systems in the United States. It is a system that processes payments and moves money between financial institutions. There are currently two network operators, Electronic Payments Network and FedACH (owned by the Federal Reserve Banks). The ACH system is used for payments such as: direct deposit, government benefits delivery, bill pay, and transfers between consumers and businesses, among others. The rules for ACH networks are set by NACHA — a private, not-for-profit, industry association. Importantly, by rule, only insured depository institutions are allowed access to the ACH networks.

According to NACHA, in 2017 ACH networks processed approximately 21.5 billion transactions with a total value of about $46.8 trillion.[556] An originator — which could be an individual or an entity — first provides payment instructions that then enter the banking system. ACH

Figure C3: Distribution of Core Noncash Payments by Type for 2015



Note: Debit card includes non-prepaid debit, general-purpose prepaid, private-label prepaid, and electronic benefit transfers. Credit card includes general purpose and private label. Check, automated clearinghouse (ACH) credit transfers, and ACH debit transfers include interbank and on-us.
Source: Federal Reserve System, *The Federal Reserve Payments Study 2016,* at 3.

555. See generally NACHA, *ACH Network: How It Works*, available at: *https://www.nacha.org/ach-network*.

556. NACHA, *2017 ACH Network Volume & Value*, available at: *https://www.nacha.org/system/files/resources/ACH-Network-Volume-and-Value-2017_2.pdf*.

payments are processed in batches by banks — the originating financial institution aggregates payment information into batches before sending to the two network operators who then net and route payments to receiving financial institutions. ACH payments can be either debit (pull)[557] or credit (push)[558] payments. Debit payments settle in one day while credit payments settle in one to two days. In 2015, ACH transferred the highest value of payments among retail payment options.

Wire Transfer Services

Wire transfer services are systems that are primarily used for large value, wholesale payments between banks and businesses. In the United States, there are two primary wire service networks that operate domestically — Fedwire and CHIPS. Fedwire is owned and operated by the Federal Reserve Banks; CHIPS is a competing private sector network with 50 direct bank participants.[559] Unlike the ACH networks, the wire networks' operating rules are set by the operators themselves.

Fedwire is a real time gross settlement service that clears and settles transactions immediately. In 2017, Fedwire processed over 150 million transactions with a total value of over $740 trillion; the average Fedwire transaction value was $4.85 million.[560] In comparison, CHIPS is a real-time final settlement system that matches, nets, and settles payments. In order to function in real time, member banks must prefund (using Fedwire) a joint CHIPS account at the New York Federal Reserve Bank. In 2017, CHIPS processed over 112 million transactions with a total value of over $393 trillion; the average CHIPS transaction value was $3.49 million.[561]

Checks and Cash

Checks and cash are two other ways to make payments. Checks are cleared in one of five ways:[562] (1) clearing "on-us" checks internally on a bank's own books; (2) presenting checks directly to the paying bank; (3) forwarding checks to a correspondent bank; (4) exchanging checks through a private clearinghouse; (5) forwarding checks to the Federal Reserve for processing. Today, nearly all of the checks that the Federal Reserve processes are electronic images of the paper checks.

---

557. For example, when a consumer pays a utility bill by authorizing the utility company to pull the payment from his or her bank account. This could be done by visiting the company's website to input payment information, for instance.

558. For example, when a consumer logs on to his or her bank's online banking portal and schedules an online bill pay transaction that the bank will then push to the payee.

559. See Fedwire at *https://www.frbservices.org/financial-services/wires/index.html* and CHIPS at *https://www.theclearinghouse.org/payment-systems/chips*.

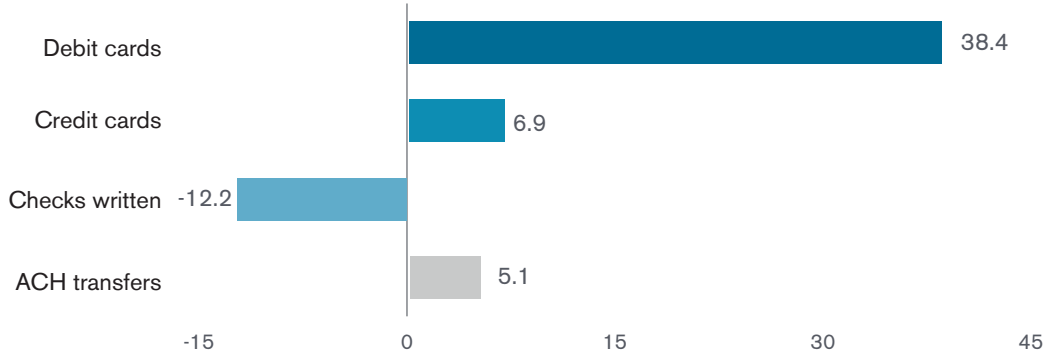
560. Board of Governors of the Federal Reserve System, *Fedwire Funds Service – Annual* (2018), available at: *https://www.federalreserve.gov/paymentsystems/files/fedfunds_ann.pdf*.

561. The Clearing House, *Annual Statistics from 1970 to 2018* (2018), available at: *https://www.theclearinghouse.org/-/media/tch/pay%20co/chips/reports%20and%20guides/chips%20volume%20through%20jan%202018.pdf*.

562. Federal Reserve Bank of New York, *Check Processing* (Mar. 2013), available at: *https://www.newyorkfed.org/aboutthefed/fedpoint/fed03.html*.

Check usage has been declining since the 1990s and continues to decline.

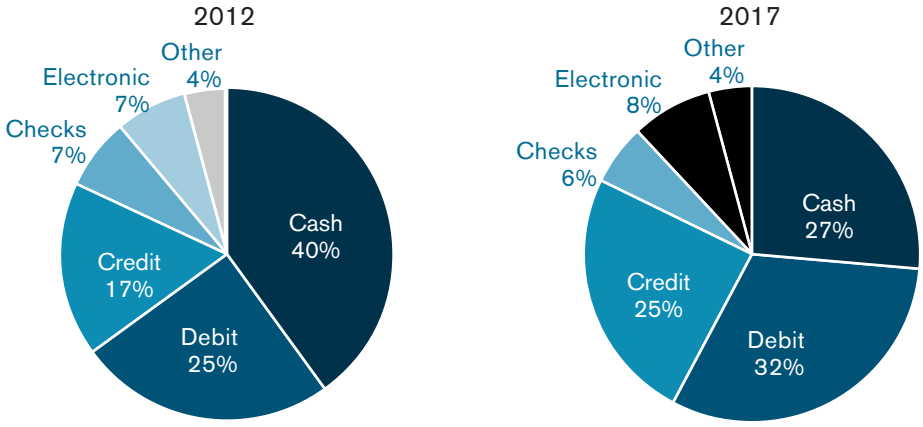
Figure C4: Changes in the Number of Consumer Noncash Payments Per Household, Per Month, 2000-2015



Note: ACH is automated clearinghouse. Debit card includes non-prepaid debit, general-purpose prepaid, and private-label prepaid (including electronic benefits transfers). Credit card includes general purpose and private label.
Source: Federal Reserve System, *The Federal Reserve Payments Study 2016*, at 4.

Cash is still the most frequently used payment method, however, its share of total payments is declining.

Figure C5: Transactions by Each Payment Instrument (percent)



Source: Surveys of Consumer Payment Choice, 2012 and 2017, Federal Reserve Bank of Boston.

Other Payments Players

In addition to the core payment systems that connect financial institutions with other financial institutions, there are a number of nonbank firms that serve as intermediaries and layer between the banking system and the ultimate end user. In some cases, other intermediaries may also layer on top or beside these intermediate firms to provide a specific or supplementary specialty service (such as tokenization, for example), which adds to the complexity of the payments system. This

section provides only a brief, high-level overview of the general categories of players in this space. While not always the most well-known, these firms provide crucial services to connect end users.

Nonbank Payment Processors

Payment processors are generally nonbank technology companies that provide vendor services to bank clients by processing electronic payments. These firms specialize in processing card payments on both sides of a transaction — as merchant acquirer and/or issuer processor. Some banks process their own payments in-house; some banks enter into a co-owned joint venture with a payment processor, whereby the processor supplies the technology to process payments and the bank maintains the merchant relationships; many banks wholly outsource the processing function to a third-party processor.[563] The role of processors in the payments ecosystem is best understood through the outsourcing model. Here, the processor in essence stands in the shoes of the acquiring bank and/or the issuing bank during the authorization, routing, and clearing of card transactions.[564]

Since payment processors are nonbank institutions, they must have a bank sponsor in order to access the card networks. Processors must follow the rules of the card networks, and are examined regularly by the networks. Processors are also examined by the banking agencies through uniform FFIEC guidance under the bank regulators' Bank Service Company Act authorities; however as these authorities regulate the third-party and vendor services that are provided to the bank, the bank sponsors are generally responsible for the processors' conduct when processing on the card networks.

Payment processing is a very competitive business that is largely driven by the firm that can charge the lowest fees. Processors themselves have diversified and tried to gain a competitive advantage by engaging in related businesses that include products and services such as: prepaid cards, PIN debit network ownership, providing hardware (such as payment terminals), and providing software solutions for small businesses (such as for accounts and inventory management, etc.).

Payment Service Providers (PSPs)

Technology has allowed new entrants to enter the business of accepting and processing merchant's and consumer's point of sale or online/mobile payments. In many cases, these firms are serving small businesses who may not have merchant relationships with banks, or compete with bank services through the quality of the software and user experience. PSPs are generally nonbank technology companies that are responding to customer demand for faster, more convenient services for both end users and merchants.

While PSPs provide merchants, for example, with a way to accept and process payments, they do not directly compete with traditional payment processors — instead they function as yet another

563. Office of the Comptroller of the Currency, *Merchant Processing, Comptroller's Handbook* (Aug. 2014), at 2-5, available at: *https://www.occ.treas.gov/publications/publications-by-type/comptrollers-handbook/merchant-processing/pub-ch-merchant-processing.pdf*.

564. See, e.g., First Data Corporation, *Form 10-K Annual Report* (Feb. 20, 2018), at 6-7, available at: *https://www.sec.gov/Archives/edgar/data/883980/000088398018000006/a12311710-k.htm*.

layer.[565] As nonbank entities, PSPs also do not have direct access to the payment infrastructure and therefore must have a business relationship with a bank. There may also be a traditional nonbank payment processor between these firms and their bank for payment processing purposes. Since PSPs layer on top of the existing payments infrastructure, they are disrupters more on the front-end consumer-facing side of user experience than on the back-end processes affecting the ultimate movement of money.

PSPs, like payment processors, must adhere to the rules of the card networks, even if they rely on banks and payment processors to process transactions through the system. To be a service provider for a card network, a firm generally must register with the card network, ensure that they are PCI-DSS compliant, and be examined annually by the card network.[566] Additionally, PSPs are generally licensed money transmitters and are therefore subject to the applicable licensing, registration, and oversight requirements in multiple jurisdictions.

565. See, e.g., Square, Inc., *Form 10-K Annual Report* (Feb. 27, 2018), at 9-11, 19, 22, available at: *https://www.sec.gov/Archives/edgar/data/1512673/000151267318000004/a10-kfilingsquareinc2017.htm*; PayPal Holdings, Inc., *Form 10-K Annual Report* (Feb. 7, 2018), at 15, available at: *https://www.sec.gov/Archives/edgar/data/1633917/000163391718000029/pypl201710-k.htm*.

566. See, e.g., Visa, *The Visa Payment Facilitator Model: A Framework for Merchant Aggregation* (May 2, 2014), available at: *https://usa.visa.com/dam/VCOM/download/merchants/02-MAY-2014-Visa-Payment-FacilitatorModel.pdf*, and Mastercard, *What Service Providers Need to Know About PCI Compliance*, available at: *https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/service-providers-need-to-know.html*.

2018-04417 (Rev. 1) • Department of the Treasury • Departmental Offices • www.treasury.gov