The Cutting Edge of Finance:

An Examination of the Work of Republicans on the House Financial Services Committee's Task Forces on Financial Technology and on Artificial Intelligence.

April 20, 2021

Hon. Patrick McHenry | Ranking Member
Committee on Financial Services

Hon. Tom Emmer | Ranking Member
Task Force on Financial Technology

Hon. Barry Loudermilk | Ranking Member
Task Force on Artificial Intelligence

Hon. French Hill | Ranking Member
Subcommittee on National Security, International Development,and Monetary Policy

Table of Contents

Executive Summary

The rapid expansion of technology in financial services has made it possible for more Americans to have access to our financial system. The current COVID-19 public health crisis has only accelerated this trend as more digital tools have been adopted by more Americans. That means that technology is playing an increasingly important role in the way that Americans transact financially, including: sending and receiving money, paying bills, accessing their accounts, obtaining a mortgage, saving and investing, and finding much-needed emergency relief during COVID-19, including the Paycheck Protection Program (PPP).

This report summarizes the work of Republicans on the House Financial Services Committee's two task forces focused on financial innovation: the Task Force on Financial Technology and the Task Force on Artificial Intelligence. The task forces were intended to help the Committee on Financial Services better understand the latest technology developments in financial services.

This report summarizes the key topics on which Committee Republicans focused, the themes that emerged over the course of the Congress, and policy recommendations for regulators and Congress. The key takeaways are that Congress must (1) promote greater financial inclusion and expanded access to financial services, and (2) ensure that the federal government does not hamper the U.S.' role as a global leader in financial services innovation. The following provides a summary of the major trends and key issues identified in this report, as well as three policy recommendations.

Digital Payments

Thanks to advances in new payments technologies, consumers have a number of options for making purchases online and at retail locations. As more businesses and consumers adopt digital payments, policymakers and regulations have an important role in making sure that America's payments system is faster and more secure in the future. Congress should continue oversight of the Federal Reserve's FedNow program to ensure that private sector innovation is encouraged. In addition, Congress should better understand the increasing role that blockchain and digital currency play in the payments space. As countries like China continue to develop their own digital currencies, the development of an American digital currency will play a pivotal role in the continued dominance of the U.S. dollar in international markets. While the development of the digital dollar is vitally important for American competitiveness, attempts to socialize our payments system through the creation of consumer accounts at the Federal Reserve may pose a threat to our civil liberties, would fundamentally alter the role of the Federal Reserve, and would crowd out private sector innovation—all of which must be avoided in the creation of an American central bank digital currency.

The AI Frontier

The use of artificial intelligence (AI) has accelerated in the past few years in various segments of the economy, including financial services. The potential impact of AI in financial services is vast in terms of how the technology is used and the industries where it can be deployed. AI and machine learning technology can help financial services companies that are facing significant strain in meeting the demands of regulatory compliance by automating what are currently manual processes. The use of AI and algorithms can also enable stronger fraud detection and prevention strategies and use of AI can offer financial services to a wider array of consumers. However, explainability behind the AI technology is important and requires transparency into what data is used, how these decisions are being made, and whether the automation leads to better results. Attempts to alter AI technology as a way to implement a socially progressive agenda has the potential to create a dangerous distraction from an otherwise highly promising innovation. America must focus on ways to foster and advance AI in a responsible manner to compete against authoritarian state actors, including China.

Protecting Consumer Data

The collection, use, and sharing of massive troves of consumer financial data allows financial firms to provide substantial improvements in how financial services are delivered and consumed. However, it also creates new areas of risk. Technology-enabled financial services companies are increasingly relying on cloud computing for their data storage and processing needs. While the use of cloud service providers offers benefits to financial institutions and consumers alike, there is an opportunity to provide greater regulatory certainty with regards to the oversight of third-party cloud service providers. Moreover, to stay ahead of bad actors, it is critical that policymakers modernize the way American citizens interact with financial institutions, including discontinuing the outdated use of Social Security numbers to identify and verify consumers. The federal government should collect consumers' financial data only when absolutely necessary, especially if the data is stored in a centralized location that is more vulnerable to cyberattacks.

Recommendations

America Must Lead in Global Payments: As China and other foreign nations look to build their own digital currencies, including central bank digital currencies, it is critical that the United States maintain its status as a global leader in payments. International trade depends on the dollar. Congress should reach consensus on how to support innovation, especially private sector innovation that builds stronger, more effective payment systems.

Automation Leads to Better Decision Making: Banks should harness the power of data and machine learning to combat fraud, streamline compliance, and make better underwriting decisions. At the same time, they must be transparent. AI cannot be a black box for how decisions are made. Instead, automating these processes requires transparency into what data is used, how these decisions are made, and whether the automation leads to better results.

Congress Must Keep Up with Technology to Better Protect Consumers: Financial services is one of the most heavily regulated industries. However, regulations must be updated to reflect the shift toward digitization. That means greater protections for consumers and their data from cyberattacks and data breaches. This also includes modernizing the way individuals are identified to ensure the minimal amount of data is used to authorize access to financial products. Congress should also examine how technology is being used to aggregate consumer financial data and modernize statutes such as the Graham-Leach-Bliley Act to ensure consumers can control how their data is used.

II. The Importance of Financial Technology to The Financial Services Industry in the 21st Century

This report underscores the important role financial technology, including artificial intelligence, plays and will continue to play in the delivery of financial services to Americans.

In 2019, the House Financial Services Committee created two new task forces to better understand the opportunities and challenges created by the use of financial technology ("fintech") and artificial intelligence ("AI") in financial services. Committee Republicans have long advocated for the Committee's review of financial innovation and supported these efforts.

Fintech and AI are areas in which policymakers can and should come together in helping to build a better, more inclusive, banking system for America. The balance policymakers must strike is to nurture the new uses of technology while ensuring core principles of safety and soundness are maintained. Advances in machine learning, quantum computing, and more broadly innovation happening across the American economy require a change in mindset in how these new technologies are addressed.

The reality is change is happening whether American policymakers are ready or not. Advances in technology and digitalization are happening in nearly every aspect of financial services, including: banking, payments, cryptocurrencies, remittances, lending, personal finance, asset management, payroll and benefits, accounting, credit scoring, insurance, and real estate. According to a 2018 report from the U.S. Department of the Treasury,

> 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. In the aggregate, the financing of such firms has been growing rapidly, reaching $22 billion globally in 2017, a thirteen-fold increase since 2010. Significantly, lending by such firms now makes up more than 36% of all U.S. personal loans, up from less than 1% in 2010.[1]

As technology advances and new banking products are developed, consumer financial information is increasingly digitized. In the same report, Treasury notes that "[b]y 2020, digitized data is forecasted to be generated at a level that is more than 40 times the level produced in 2009."[2] Further, Treasury found that "[t]oday, 50% of people with bank accounts use mobile devices to

[1] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, United States Department of the Treasury, 5, https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf
[2] *Id.* at 8.

access their information, up from 20% in 2011, while the number of physical bank branches has been declining since 2009."[3]

As banking services become increasingly digital, our financial markets are seeing unprecedented global connectivity. This globalization is a boon not just for the development of new, innovative financial products, but has led to an expansion of consumer access to traditional financial services, particularly for communities that have historically been un- and under-banked. It has also posed many questions and challenges the financial services industry has not considered in the past. The issue for Congress is how to meet these challenges and opportunities in this new world of financial services while ensuring consumers are protected.

America was built on ingenuity and on generations of entrepreneurs and innovators. Testing, tinkering, and iterating led us to where we are today. Not only is financial innovation a critical part of our nation's history, but it is what makes it easier for all Americans to participate in our financial system. From saving for college to accessing capital to start a small business, we need a more modern banking system that meets the needs of today's American consumer. In short, Washington, D.C. must not and cannot be a place where financial innovation goes to die.

For Congress, the AI and fintech task forces represent a massive opportunity to better understand the rapid changes that are taking place in our financial system, and to work towards achieving a consensus on practical solutions for meeting the challenges of that future together. These task forces can assist in helping to create a better regulatory framework to meet the demands of these new technologies. Yet, policy decisions must be based on data, not fear.

If history is a guide, it is better to be on the side of American innovation, competition, and most importantly the freedom to build a better future for all of us. If the current global pandemic has taught us anything, it is that progress is not preordained. Technologies that prior to 2020 were viewed as mere convenience are now necessities to everyday life.

Congress should look to the next frontier of innovation and how to help the builders of the future. This includes how we foster and support financial innovation that makes our system faster, safer, and more inclusive for more Americans.

---

[3] *Id.* at 18.

III. Current and Future Challenges for Financial Innovation

A. Digital Globalization: Wholesale and Real-Time Payments, and Digital Currencies

i. Wholesale and Real-Time Payments

U.S. Payment System

Millions of payment transactions are processed each day in the United States.[4] Credit and debit cards remain the leading point of sale methods in the United States,[5] while the number of digital wallet transactions in the United States has increased 41 percent from nearly $70 billion to nearly $100 billion in the past two years alone.[6] The sheer volume of payment transactions has marked a turning point in the speed in which consumers expect their transaction to complete. Central to the faster payment discussion is payments infrastructure, the process by which banks send money to each other. Transactions within a single bank are fairly straightforward. Two consumers who bank with the same institution are able to transfer funds quickly because there is no settlement with another bank; the transaction simply registers as an update on the bank's accounting system.

Bank-to-bank transactions are more complex. Customers at Bank A who want to send money to customers at Bank B are disadvantaged if the respective customers do not have a business relationship with the other's bank. There must be some kind of business relationship between the two banks to allow the transaction to occur. One solution is for Bank A to hold an account at Bank B and settle the transaction internally. This is known as a correspondent banking relationship in which the two banks have commercial banking accounts to allow their customers to make payments with one another. However, such an arrangement requires that banks have a direct relationship. If the two banks do not have a direct relationship, another intermediary is needed for the banks to coordinate these transactions and process these requests within a secure, organized way.

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) is an example of such intermediary. SWIFT is a network that allows banks to securely exchange electronic transactions with one another through payment orders. Each financial institution sends financial

---

[4] *Fueled By Increased Consumer Comfort, Mobile Payments In The U.S. Will Exceed $130 Billion In 2020*, Forbes (Mar. 1, 2020), https://www.forbes.com/sites/shelleykohan/2020/03/01/fueled-by-increased-consumer-comfort-mobile-payments-in-the-uswill-exceed-130-billion-in-2020/?sh=5613934444f2; *Commercial Automated Clearinghouse Transactions Processed by the Federal Reserve--Annual Data*, Board of Governors of the Federal Reserve System, https://www.federalreserve.gov/paymentsystems/fedach_yearlycomm.htm.

[5] *Leading point of sale payment methods in the United States in 2019*, Statista, https://www.statista.com/statistics/568523/preferred-payment-methods-usa/.

[6] *Fueled By Increased Consumer Comfort, Mobile Payments In The U.S. Will Exceed $130 Billion In 2020*, Forbes (Mar. 1, 2020), https://www.forbes.com/sites/shelleykohan/2020/03/01/fueled-by-increased-consumer-comfort-mobile-payments-in-the-uswill-exceed-130-billion-in-2020/?sh=5613934444f2.

messages on SWIFT that provide instructions to the corresponding banks to debit and credit accounts.

SWIFT has helped manage the flow of information between banks to make transactions faster, more secure, and automated. However, questions remain about the calculation of risk, including the appropriate amount of funds a bank's commercial account must maintain in order to settle the enormous number of transactions.

To address the uncertainty, banks created clearinghouses operating under a deferred net settlements system. Under the deferred net settlements system, banks do not have to maintain a large amount of cash on deposit or settle each small payment in real time. Instead, when the bank receives a request to debit or credit an account, the bank records and transmits the transaction to a central clearinghouse, which tracks of all the payments. At the end of the set period of time, the banks settle the amounts of money they owe one another that the clearinghouse has been recording.

This system was built by The Clearing House and the Federal Reserve, which created the core payments infrastructure for the United States' payments system operators. The National Automated Clearing House (NACHA) is the administrator of this system and is responsible for setting and enforcing the rules of payments.

The Reserve Banks and The Clearing House's Electronic Payments Network (EPN) are the two national Automated Clearing House (ACH) operators. The Reserve Banks and EPN rely on each other to process "inter-operator ACH payments," or payments for which one bank is on EPN and the other is operated by a Reserve Bank. This system helped to create other mechanisms for banks to move away from cash and checks and toward more modern models, like direct deposits and online payment options. For example, the Clearing House Interbank Payments System (CHIPS) is used for large-value transactions. CHIPS clears and settles $1.5 trillion in domestic and international payments per day. Fedwire is the Fed counterpart to CHIPS and has close to 10,000 participants.

U.S. Payment System Compared to Rest of the World

The issue of timely payments centers on the mechanisms by which consumers transfer funds and how quickly the recipient can access those funds. Consumers embrace mobile banking as a way of making payments at the click of a button. However, in the United States, the infrastructure on the backend of those transactions is antiquated. It often takes one to two business days, excluding holidays, weekends, and evenings to complete a transaction. Compared to the rest of the world, the U.S.' payment system is one step behind. More than 20 countries already have real-time payment systems, including: the United Kingdom, Mexico, and Switzerland.

There are several reasons why the United States lags behind other countries as it relates to payment systems. The first is a lack of incentives. Banks maintain a "float period," during which time the money is committed but not yet paid. Banks can invest those funds during that time period to earn

returns. For smaller banks and credit unions in particular, a loss of returns during the float periods could materially hurt their bottom line. It will also be difficult and expensive for operators to build a new infrastructure that would allow for real-time payments.

Another reason is security. Account takeover fraud allows bad actors to control the accounts of users and send money before the legitimate holders notice the funds missing. The current system of delayed payments processing and settlements allows the clearinghouses and banks time to identify these types of fraudulent transactions. This in turn allows transactions to be cancelled before they are finalized. Under a real-time payment paradigm, account takeover fraud poses a particularly troubling risk because transactions are cleared instantly and irrevocably. As a result, criminals are able to move money more quickly from account to account, and then extract it immediately.

Consumer Demand

Notwithstanding these concerns, the demands of a more mobile and digital economy have led consumers to expect faster, real-time payments. As a result, larger banks have invested more than $1 billion in a new real-time payments system. In November 2017, the Clearing House announced the launch of its Real-Time Payments Network, RTP. To date, sixteen banks have joined RTP, and together represent just over half of all the accounts for which payments can be made. More recently, the Fed announced a new service called FedNow that will allow 24/7 real-time payments services. It is expected to launch in 2023 or 2024.

FedNow

In September 2019, the Task Force on Financial Technology held a hearing on the future of real-time payments. Two key issues emerged for a U.S. real-time payment system: interoperability and ubiquity.

Carol Benson, Founding Partner of Glenbrook, testified that the success of a real-time payments system is dependent on its accessibility, affordability, security, and ubiquity. Most countries around the world have achieved ubiquity by pursuing a single, national system. In the United States, the entrance of FedNow, in addition to private sector alternatives, creates the potential for a multi-provider model. Thus, to achieve ubiquity in a multi-provider system, the providers must have interoperability, or connectivity between distinct providers.

Interoperability is not solely an issue of technical capability, but one of governance. In a multi-provider system, it is vital that the relevant actors are subject to a single set of rules. Ms. Benson further testified, “[a] common governance structure would also ensure that the industry works together – rather than in separate and fractious groups – on issues such as transaction security,

payments addressing, and the ability to eventually connect to other countries."[7] Whatever system the United States adopts, interoperability will be key to its proper functioning.

In October 2020, the Federal Reserve announced the launch of the FedNow Pilot Program through which financial institutions can participate in discussions and demonstrations to test the service. The Federal Reserve remains committed to a 2023–2024 launch of FedNow.

The Fed's decision to create its own real-time payments infrastructure is not without controversy. In fact, the Fed's Vice Chairman of Supervision, Randal Quarles, disagreed with the Fed's decision to proceed with the plan, stating the Fed's decision would "crowd out innovation when viable private-sector alternatives are available."[8] Critics echo Vice Chair Quarles' concerns suggesting the existence of FedNow will discourage competition in the private sector.[9]

Additionally, the Fed's entrance into the market as a competitor results in an inherent tension with its responsibilities to regulate. Critics are concerned that the regulatory arm of the Federal Reserve could be weaponized in order to support the success of the FedNow program to the detriment of the financial system. Under Title VIII of Dodd-Frank, the Clearing House is designated as a Systemically Important Financial Market Utility. This status subjects it to enhanced regulatory oversight.

Proponents of the FedNow program argue the private sector failed to step in to provide real-time payment solutions until the Fed acted. Proponents contend that without the Fed's involvement, a monopoly will be created for payments. Moreover, smaller financial institutions and community banks are optimistic a FedNow program will lead to greater access and affordability for faster payments.

Financial inclusion is also a big driver of the FedNow program. Aaron Klein from the Brookings Institute observed for Americans living paycheck to paycheck, waiting up to six days before the money is available is a serious problem if rent, utilities, child support, car payments become due before then.[10] Real-time payments will mean that American families would no longer have to wait to get access to funds that are, after all, already theirs.

---

[7] *The Future of Real-Time Payments: Hearing Before the Task Force on Financial Technology of the H. Comm. on Financial Services*, 116th Cong., (Sept. 26, 2019), *available at* https://docs.house.gov/meetings/BA/BA00/20190926/110016/HHRG-116-BA00-Wstate-BensonC-20190926.pdf.
[8] *Fed to Create Payments System to Speed Money Transfers*, Wall Street Journal (Aug. 5, 2019), https://www.wsj.com/articles/fed-to-create-payments-system-to-speed-money-transfers-11565026200.
[9] *UPDATE: Fed developing faster payments service to rival big banks' network*, S&P GLOBAL (Aug. 5, 2019), https://www.spglobal.com/marketintelligence/en/news-insights/trending/rfEUCxA6IkIkU_8OmjMQWA2.
[10] *How the Fed can help families living paycheck to paycheck*, Brookings (Nov. 22, 2017), https://www.brookings.edu/research/how-the-fed-can-help-families-living-paycheck-to-paycheck/.

Still, questions remain whether the existence of FedNow will create a government monopoly and stymie existing private sector efforts of a faster payments system. While proponents of the initiative like Federal Reserve Board Governor Lael Brainard claim that FedNow is not intended to stifle competition,[11] such assurances do not square with the wider central bank policy discussions on the benefits of public payment options. For example, a recent report by the Bank of International Settlements highlighted that one of the key "benefits" to a public payments system like FedNow is that it eliminates the need for private sector innovations like stablecoins:

> Some of the benefits also could be achieved through less far-reaching reforms to existing payment systems. For instance, retail fast payment systems (FPS) may allow for the 24/7 availability and speed that consumers and businesses are demanding. It may also be possible to program payments in such a way as to support atomic settlement (immediate "delivery-vs-payment"), to allow for very small values (micro- payments) or to be interoperable with [Digital Ledger Technology] DLT systems. Together with advances in digital ID, such systems could also work to enhance financial inclusion and universal access (Arner et al., 2018). Indeed, the recent experience with the India Stack (D'Silva et al., 2019) shows that great strides can be achieved through public payment and other infrastructures that do not rely on DLT, stablecoins or [Central Bank Digital Currencies] CBDCs. Unlike CBDCs, FPS build on existing accounts at intermediaries. Such accounts are not backed by the sovereign, but they also do not lead to concerns around "digital runs" or disintermediation.[12]

And despite Governor Brainard's past assurances to the contrary, her most recent remarks track this BIS framework of promoting public payments initiatives like FedNow to the detriment of private sector innovation.[13] Specifically, she casts doubt to the "legal and regulatory" status of stablecoins, while proclaiming that the Federal Reserve remains "committed to building an instant payment system that delivers the payment speed that users want." This is a striking endorsement of a public payment option framed in direct competition to a private sector innovation. It is particularly troubling given that the Fed *itself* that can determine the legal and regulatory status of its own competition.

Congress must continue oversight of the Federal Reserve's FedNow program to ensure that private sector innovation encouraged. Moreover, oversight of FedNow is necessary to ensure it is fully

---

[11] *Fed to develop real-time payments system for launch in 2023 or 2024*, Reuters (Aug. 5. 2019), https://www.reuters.com/article/usa-fed-payments/fed-to-develop-real-time-payments-system-for-launch-in-2023-or-2024-idINL2N2510UL.

[12] *BIS Working Papers No 905 Stablecoins: risks, potential and regulation*, BANK FOR INTERNATIONAL SETTLEMENTS (Nov. 2020), https://www.newyorkfed.org/medialibrary/Microsites/fmlg/files/2020/BIS_working_paper_905_stablecoins.

[13] The Future of Retail Payments in the United States, Board of Governors of the Federal Reserve system (Aug. 6, 2020), https://www.federalreserve.gov/newsevents/speech/brainard20200806a.htm.

interoperable with the private-sector instant payment service to accomplish the goal of nationwide reach for instant payments. If the government takes steps which risk stifling private sector efforts, America will continue to lag behind our peers in the real-time payments space.

ii. Digital Currencies and Blockchain Technology

Blockchain

One promising development in the financial services industry over the past decade is the use of blockchain. Blockchain technology provides a way to record and verify data through a public ledger, called a blockchain. Blockchain technology has enabled the creation of digital property, potentially revolutionizing the global economy. But the technology has also posed a number of novel legal and policy questions, owing in part to the fact that blockchain technology allows for the provision of financial services without an intermediary.

A blockchain includes a number of "blocks" linked together with a reference in each block to the previous block. Each block records transactions, which are essentially changes in the listed owner of an asset. These new blocks are added to the chain through a consensus mechanism through which members of the network confirm transactions as valid.[14]

In its simplest terms, blockchain technology can be described as "connected computers reach[ing] agreement over shared data."[15] Connected computers, called a peer-to-peer network, use an algorithm to verify transactions. Computers that verify transactions are called validator nodes. Importantly, the ledger cannot be modified after a transaction is verified, making it a trusted method of tracking and sharing data.

Blockchain systems can be public (permissionless) or private (permissioned). In permissionless blockchain systems, open source software is used, anyone can join the network, and any capable computer can act as a validator node.[16] Thus, permissionless blockchain is at its core open and decentralized. On the other hand, in a permissioned blockchain, a computer must be granted access to operate as a validator node.

---

[14] Rebecca Lewi, John W. McPartland , Rajeev Ranjan, Blockchain and Financial Market Innovation, Federal Reserve Bank of Chicago Economic Perspectives, Vol. 41, (Nov. 7, 2017), available at https://www.chicagofed.org/publications/economic-perspectives/2017/7

[15] *What is "Blockchain" anyway?*, COIN CENTER (Apr. 25, 2017), https://coincenter.org/entry/what-is-blockchain-anyway.

[16] *Blockchain for Dummies: Ultimate Blockchain 101 Guide*, CRYPTOMANIAKS, https://cryptomaniaks.com/guides/blockchain-for-dummies-ultimate-blockchain-101-guide; *Here's the difference between 'permissioned' and 'permissionless' blockchains*, THE NEXT WEB, https://thenextweb.com/hardfork/2018/11/05/permissioned-permissionless-blockchains/.

Digital Assets and Blockchain

Blockchain is the underlying technology for most digital assets. Digital assets, which can serve as a medium of exchange like the U.S. dollar, are not legal tender and are generally not currently backed by any government entity. The technology supporting digital assets is based on public key cryptography that protects against unauthorized access or use. Moreover, since the network is decentralized, parties can transact without the use of a central party to validate the transactions.

Digital assets provide a new medium of exchange. But the market is continuously evolving. For example, the first digital asset – Bitcoin – was launched in 2009. Since then, the market has continued to grow. Yet, governments around the world have responded differently with different regulations of digital assets. Additionally, in the United States, the U.S. Securities Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) each have jurisdiction over digital assets, with primary jurisdiction depending on whether the asset is considered a security or commodity respectively. This is in addition to a number of states that have passed legislation regulating cryptocurrencies.

Securities Law

The SEC has defined many purported cryptocurrencies and other digital assets as securities offerings. Central to the SEC's analysis is determining whether the digital asset to be issued is an "investment contract," thus making it a security. For those offerings the SEC deems to be a security, such as with many "initial coin offerings", the SEC has brought a number of enforcement actions against issuers of such tokens for (among other points) failure to register a security prior to its sale.[17]

To provide guidance to the industry, the staff of the Division of Corporation Finance at the SEC issued a non-binding advisory letter entitled "Framework for 'Investment Contract' Analysis of Digital Assets" (the Framework) to guide potential digital asset issuers in determining whether U.S. federal securities laws are applicable to their offering.[18] While the Framework is only SEC staff guidance, it is widely viewed as the broader framework that the SEC uses in determining when to bring enforcement actions against issuers of digital assets.

Under the Framework, the SEC staff uses the test established by the Supreme Court in *SEC v. W.J. Howey Co.*, as a guide in determining whether an asset is an "investment contract."[19] In particular, the relevant question is whether the asset was purchased by a holder with the "reasonable

[17] *See* examples of SEC enforcement actions at https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.
[18] *Framework for "Investment Contract" Analysis of Digital Assets*, U.S. SECURITIES AND EXCHANGE COMMISSION, available at https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.
[19] *Id.*

expectation of profits derived from the efforts of others."[20] The analysis focuses on the "efforts of others" and whether there is a group of people or entities upon which the digital asset relies. Additionally, the SEC has issued a no-action letter to a company using blockchain and digital token technology for chartering private air travel.[21] In addition, the SEC approved a Regulation A+ offering for a company to sell digital tokens on its software platform.[22]

Congress should encourage the SEC and the CFTC to build on its Framework and provide more guidance and certainty to the industry. Congress may do so by encouraging innovation labs or other offices at the regulators, and should consider creating cross-agency working groups to facilitate regulatory development.

Custody of Digital Securities by Broker-Dealers

Broker-dealers seeking custody of digital securities must comply with Securities Exchange Act Rule 15c3-3. Also known as the Customer Protection Rule, Rule 15c3-3 safeguards customer securities to prevent loss or harm in the event of a firm's failure. At its core, the Customer Protection Rule requires a broker-dealer to promptly obtain and thereafter maintain physical possession or control of all fully-paid and excess margin securities it carries for the account of customers.[23] As the market for digital securities is constantly evolving, uncertainty remains around the application of the Customer Protection Rule. Specifically, there is legal uncertainty around the ability to hold possession or control with respect to the custody of digital securities for customers by broker-dealers.[24]

To alleviate that uncertainty, in December 2020 the Division of Trading and Markets at the SEC issued a statement providing relief from enforcement relating to the Customer Protection Rule for five years for brokers transacting in digital assets. Relief is available if the broker-dealer complies with the circumstances in the statement to mitigate risk, on the basis that the broker-dealer deems itself to have met certain obligations to maintain possession or control of the applicable digital assets. In addition, the SEC posed specific questions for comment from industry participants and others in the general public to gain additional insight to help guide any future rulemaking or action.[25]

---

[20] *Id.*
[21] Response of the Division of Corporation Finance, U.S. SECURITIES AND EXCHANGE COMMISSION, https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.
[22] *SEC Clears Blockstack to Hold First Regulated Token Offering*, WALL STREET JOURNAL (July 10, 2019), https://www.wsj.com/articles/sec-clears-blockstack-to-hold-first-regulated- token-offering-11562794848
[23] *See* 17 CFR 240.15c3-3(b).
[24] SEC and FINRA Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities, available at https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.
[25] SEC Statement and Request for Comment Regarding the Custody of Digital Asset Securities by Special Purpose Broker-Dealers, available at https://www.sec.gov/rules/policy/2020/34-90788.pdf. Among other requirements, to be eligible for relief under the statement, a broker-dealer must limit its business to digital asset securities, establish and implement policies and procedures reasonably designed to mitigate the risks associated with conducting a

Congress and the SEC should monitor the implementation of the SEC's broker-dealer custody relief, and each should consider extending relief to other financial services providers such as investment advisers.

Virtual Currencies Law

Even if a digital asset is not a security, it still may be a "virtual currency" and subject to CFTC regulation. The CFTC also has oversight over futures, options, and derivatives contracts, including those for which the underlying asset is a virtual currency.

Federal courts have issued orders holding the CFTC has the power to prosecute fraud involving virtual currency. To that end, the CFTC has issued a number of Customer Advisories on topics relating to virtual currencies. These advisories address the risks associated with buying so-called "utility coins" or "consumption tokens" and the risks associated with virtual currency derivative products. The Commission also recently issued interpretive guidance to provide additional clarity regarding "actual delivery" of virtual currencies.[26]

Anti-Money Laundering Law

Financial institutions are required, under the Bank Secrecy Act (BSA), to take certain steps to verify customer identities in order to prevent fraud and money laundering. These requirements are referred to as Know Your Customer (KYC) and anti-money laundering (AML) regulations.

The introduction of digital assets poses further challenges to AML and other programs to target bad actors, particularly as digital asset use becomes more ubiquitous. Blockchain has the advantage of being a secure, non-modifiable ledger of transactions. Yet, the anonymity afforded to holders of digital assets presents challenges to KYC requirements. In May 2019, FinCEN released guidance on the application of these regulations to virtual currencies. However, it did not establish any new requirements.[27] As digital assets continue to proliferate and adoption becomes more widespread, Congress must act to ensure that digital assets and virtual currencies do not become a safe haven for bad actors.

---

business in digital asset securities, and provide customers with certain disclosures regarding the risks of engaging in transactions involving digital asset securities. *See id.*

[26] *See* CFTC Press Release, "CFTC Issues Final Interpretive Guidance on Actual Delivery for Digital Assets" (Mar. 24, 2020), available at https://www.cftc.gov/PressRoom/PressReleases/8139-20.

[27] *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FINCEN (May 19, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

Libra

One of the most high-profile examples of virtual currency was the Libra project launched by Facebook. In June 2019, Facebook Inc. announced the formation of Calibra, a Facebook subsidiary, as well as plans to introduce a digital wallet for Libra, a new cryptocurrency, and payment system. Facebook described Libra as a "new global currency powered by blockchain technology." Facebook announced that the cryptocurrency would be launched through the Libra network in 2020. At the time of the announcement, Libra released a white paper, which explained the project in more detail.

However, in the wake of the announcement of Libra, Congress and regulators expressed concerns about how the cryptocurrency would be used and regulated. Critics voiced further skepticism that Libra could meet its goal of launching in 2020. In October 2019, the Department of Treasury sent a letter to several of the founding members in the payments industry inquiring about their money-laundering compliance programs and how their involvement in Libra would comport with those policies.

On July 17, 2019, the Committee held a hearing examining Libra. While that hearing was a first step to understand the many issues that accompany a project of this magnitude, Congress still has a long way to go in understanding the implications of Libra. Financial Services Committee Democrats attached a discussion draft entitled Keep Big Tech Out of Finance Act, which would prohibit big tech companies from being, or being affiliated with, financial institutions.

When Libra was announced, 28 companies joined as "founding members" by signing a nonbinding letter of intent to join the Association. However, as the project drew increased scrutiny, several founding members—including PayPal, Visa, Mastercard, and Stripe—dropped out of the Libra Association before signing its charger. The Libra Association held its first council meeting in Geneva on October 14, 2019, with 21 founding members in attendance. Since then, additional members have dropped out of the project.

In April 2020, the Libra Association announced changes to the project in response to the widespread criticisms and began the process of obtaining licensing from The Swiss Financial Market Supervisory Authority (FINMA). At the time, the Libra Association stated that it still planned to launch the project by the end of 2020. However, in October 2020, the G7 announced its opposition to any global stablecoin project "until it adequately addresses relevant legal, regulatory, and oversight requirements through appropriate design and by adhering to applicable

standards."[28] In December 2020, the Libra Association announced it would change its name to "Diem," and planned to launch a stablecoin pegged to the U.S. dollar in 2021.[29]

Regardless of the outcome of the Libra project, it is clear that the proliferation of virtual currencies will continue and will bring with it many opportunities and challenges for the financial services industry. Congress should face these opportunities and challenges head on, and continue its oversight of existing and new technologies that will change the financial services landscape.

Central Bank Digital Currency

The coronavirus pandemic has only sharpened the focus on the drawbacks of America's payments system. The CARES Act provides for Economic Impact Payments (EIP) to American households of up to $1,200 per adult for individuals whose income is less than $99,000 (or $198,000 for joint filers) and $500 per child under 17 years old—or up to $3,400 for a family of four. Less than ten weeks after its passage, 91 percent of the $293 billion in EIP fund had been disbursed.

While the speed of disbursements has been a success, the programs have not been without glitches. The online tools built to facilitate payments have had a number of issues, related to user experience or quirks with the IRS's database integrations. Taxpayers who do not have their bank information on file with the IRS could not access direct deposits, nor were they sent checks in the mail. Instead, taxpayers were sent prepaid debit cards. The debit cards caused confusion, with many Americans unwittingly throwing away the cards thinking they were sent checks in the mail.

A digital dollar offers an alternative way for citizens to send and receive money, including receipt of government stimulus payments. One proposal is the creation of a United States Central Bank Digital Currency (CBDC). Creating a CBDC in the United States could offer the government another option for facilitating speed, efficiency, and effectiveness of payment. Moreover, as countries like China continue to develop their own digital currencies, the development of an American digital currency plays a vital role in the continued dominance of the U.S. dollar in international markets.

The question remains how the United States should best develop a digital dollar. On June 11, 2020, the Task Force on Financial Technology held a hearing on digital tools, including the advent of the digital dollar. In testimony provided by former commissioner of the Commodity Futures Trading Commission, the Hon. J. Christopher Giancarlo, suggested that Treasury—with the assistance of the Federal Reserve—should create a pilot program that brings together private sector

---

[28] *G7 voice concern about ransomware attacks; say stablecoin needs regulation,* REUTERS (Oct. 13, 2020), https://www.reuters.com/article/imf-world-bank-g7/g7-voice-concern-about-ransomware-attacks-say-stablecoin-needs-regulation-idINN9N2E201P.
[29] *Libra Rebrands to 'Diem' in Anticipation of 2021 Launch*, COIN DESK (Dec. 1. 2020), https://www.coindesk.com/libra-diem-rebrand.

innovation with public policymakers and regulators to develop a digital dollar.[30] The pilot program would explore how to maintain the supremacy of the U.S. dollar, develop U.S. technology to remain best-in-class for digital currency adoption, and ensure that individual privacy concerns are preserved and enhanced in the future. Policymakers should continue to explore ways that the United States can create a digital dollar that ensures America continues its dominance as the world's leading currency.

B. The AI Frontier: The Impact of Machine Learning in Financial Services

The use of artificial intelligence (AI) has accelerated in the past few years in various segments of the economy, including financial services. The concept of AI can vary, but generally it is associated with efforts to enable machines or computers to imitate and recognize aspects of repeatable and discrete operations, thereby mimicking cognitive functions commonly associated with the human mind. Examples include facial and voice recognition, natural language processing, and increasingly complex decision making in strategic games, "smart" systems, and even autonomous driving.

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 datasets to "self-improve" without being explicitly programmed by humans each step of the way. The nature of "improvement" in the software depends on the specific machine learning use-case, but may include the quality of image-recognition, the ability to more accurately identify relevant data, and the ability to better identify trends.

The potential impact of AI in financial services is vast, not only in the ways that the technology is used, but also the various industries where it can be deployed. The following highlights some of the possible use cases for AI and machine learning in financial services.

Back Office and Regulatory Efficiency

New and emerging AI technology will allow back office processes to be improved. AI and machine learning technology can help financial services companies that are facing significant strain in meeting the demands of regulatory compliance by automating what are currently manual processes. Otherwise known as regulatory technology ("RegTech"), advances in AI allow companies to automate regulatory filings, track employee compliance, and better comply with regulations such as Know Your Customer and anti-money laundering rules. AI makes it easier to cross-reference records and pull relevant data faster. In addition to saving time and money, AI can

[30] *Inclusive Banking During a Pandemic: Using FedAccounts and Digital Tools: Hearing Before the Task Force on Financial Technology of the H. Comm. on Financial Services*, 116th Cong., (June 11, 2020), *available at* https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-giancarloj-20200611.pdf.

also help manage risk. Finally, AI can be used to better capture something as granular as suspicious activities and the risk profile of a customer account, all the way to something much larger involving complex data sets for analyzing the systemic risk profile of investments and underwriting for the financial services firm itself.

Smart Finance

While still nascent, financial services firms are investing heavily in creating platforms for customers to automate decisions in everything from how we budget our money to where we invest our money. By automatically allocating across financial products that make the most "optimal" choices for the consumer, customers are allowed better personal financial management, while allowing institutions to better optimize deposits in real time.

Better Lending Decisions

Lending products rely on data that is often stored across multiple internal and external systems and is often manually entered. This can increase the number of inaccuracies and create delays—if not denials—for otherwise creditworthy borrowers. Particularly for segments of the population that are unbanked or underbanked, advanced credit-decision models can use AI to improve the confidence of lenders in extending credit, reducing defaults, and can find data that is not readily available for traditional assessments of creditworthiness. Not only is this happening in the consumer space, but AI is enabling financial institutions to provide more financing for small and medium-size businesses by streamlining the application and review process, as well as utilizing predictive algorithms to anticipate when financing is most needed and when it will be repaid.

i. The Use of Alternative Data in the Underwriting Process

The use of alternative data in underwriting decisions has emerged as one way technology can increase the accuracy of such decisions and reduce costs for both consumers and lenders. In making underwriting decisions, lenders and credit scorers have traditionally used data such as credit card, mortgage, and student loan payments to determine an individual's creditworthiness. Access to credit allows individuals to buy a car or house, pay for college, or start a small business. The use of "alternative data" – information such as education level, employment status and history, and utility bill payments – has the potential to expand access to credit to consumers that lack credit history. In particular, its use provides a more holistic picture of an individual's creditworthiness. Indeed, research indicates that the use of such data can improve an individual's credit score or enable an individual to obtain a credit score for the first time.[31]

[31] *See, e.g., Alternative Data and the Unbanked*, OLIVER WYMAN, https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2017/may/Oliver_Wyman_Alternative_Data.pdf; *Alternative Data to Develop Credit Scores*, WORLD BANK, http://siteresources.worldbank.org/FSLP/Resources/ChetWiermanski_AlternativeData.pdf.

In July 2019, the Task Force on Financial Technology held a hearing entitled "Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit." Dave Girouard, co-founder and CEO of Upstart, testified that "45% of Americans have access to bank-quality credit, yet 83% of Americans have never actually defaulted on a loan."[32] Mr. Girouard's explained that the gap "45% versus 83% gap" is due in part to outdated models for assessing creditworthiness:

> The FICO score was introduced in 1989 and has since become the default way banks judge a loan applicant. But in reality, FICO is extremely limited in its ability to predict credit performance because it's narrow in scope and inherently backward looking.[33]

The use of alternative data is one way to increase fairness in lending and expand access to credit by building more accurate credit models. While the pieces of data traditionally collected by credit reporting agencies are helpful in determining the creditworthiness of a consumer, alternative data can provide a more holistic picture of an individual's creditworthiness. Inaccurate credit scores can drive up costs for consumers, as well as exclude the borrowers deemed most risky. By considering additional data points, lenders are able to better assess risk, and consumers can access credit based on more accurate assessments. Often, the inclusion of alternative data benefits consumers. According to a study, including positive rent payments in a credit score determination could increase credit scores for 76 percent of the New York City tenants sampled, particularly in low income and minority communities.[34] Another study found that when positive utility payments were included in a credit score determination, 77 percent of individuals sampled had an increased credit score.[35]

Mr. Girouard testified to the Committee that Upstart's efforts have in fact expanded access to credit:

- "[Upstart's] model approves 27% more consumers and lowers interest rates by 3.57 percentage points, compared to a traditional lending model."[36]

---

[32] *Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit: Hearing Before the Task Force on Financial Technology of the H. Comm. on Financial Services, 116th Cong*., (July 25, 2019), *available at* https://docs.house.gov/meetings/BA/BA00/20190725/109867/HHRG-116-BA00-Wstate-GirouardD-20190725.pdf.
[33] *Id.*
[34] *Making Rent Count*, NEW YORK CITY COMPTROLLER, https://comptroller.nyc.gov/reports/making-rent-count/rent-and-credit-report/.
[35] *Let there be light: the impact of positive energy-utility reporting on consumers*, EXPERIAN INFORMATION SOLUTIONS, https://www.experian.com/assets/consumer-information/white-papers/cis-energy-utilities-tl.pdf.
[36] *Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit: Hearing Before the Task Force on Financial Technology of the H. Comm. on Financial Services, 116th Cong*., (July 25,

- "For near-prime consumers (620-660 FICO) our model approves 95% more consumers and reduces interest rates by 5.42 percentage points compared to a traditional model."[37]

Upstart is not the only entity using alternative data to achieve more accurate credit modeling. Experian, Equifax, and TransUnion have each established relationships with companies that collect alternative data.[38] LendingClub and Kabbage also use alternative data in their lending practices.[39] In a survey, TransUnion found that 34 percent of lenders are using some form of alternative data in evaluating creditworthiness. Further, the same survey found that through the use of alternative data, "66 [percent] of lenders surveyed reported that they were able to lend to additional borrowers in their current markets and 56 [percent] reported access to new markets by using alternative data."[40]

The CFPB has acknowledged the potential benefits of using alternative data. In February 2017, CFPB launched an inquiry into the benefits and risks of using alternative data in making lending decisions.[41] In announcing the inquiry, the CFPB noted that 26 million Americans have no credit history and another 19 million have an insufficient credit history to produce a credit score. According to the CFPB, the barriers to accessing credit disproportionately affect low income and minority consumers. The CFPB identified several potential advantages of using alternative data, including increasing access to credit, helping lenders better assess consumer creditworthiness, expediting the application process, and reducing costs for lenders and borrowers. The CFPB also identified several potential disadvantages, including fair lending and privacy concerns.

Following the inquiry, in September 2017 the CFPB issued a No-Action letter to Upstart Network, Inc., an online lending platform that uses "alternative data" in making credit and pricing decisions.[42] As part of the no-action letter, Upstart was required to regularly report lending and compliance information to the CFPB, in order to "further [the bureau's] understanding of how these types of practices impact access to credit generally and for traditionally underserved

---

2019), *available at* https://docs.house.gov/meetings/BA/BA00/20190725/109867/HHRG-116-BA00-Wstate-GirouardD-20190725.pdf.

[37] *Id.*

[38] *Alternative Data: The Great Equalizer To Lending Inequalities?*, FORBES (Aug. 4. 2019), https://www.forbes.com/sites/forbestechcouncil/2019/08/14/alternative-data-the-great-equalizer-to-lending-inequalities/?sh=2f1be6312449.

[39] *Id.*

[40] *Alternative Data and the Unbanked*, OLIVER WYMAN, https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2017/may/Alternative_Data_And_The_%20Unbanked.pdf.

[41] *CFPB Explores Impact of Alternative Data on Credit Access for Consumers Who Are Credit Invisible*, CONSUMER FINANCIAL PROTECTION BUREAU, https://www.consumerfinance.gov/about-us/newsroom/cfpb-explores-impact-alternative-data-credit-access-consumers-who-are-credit-invisible/.

[42] *CFPB Announces First No-Action Letter to Upstart Network*, CFPB, https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-first-no-action-letter-upstart-network/.

populations[.]"[43]

In December 2018, GAO published a report entitled "Agencies Should Provide Clarification on Lenders' Use of Alternative Data."[44] GAO found significant growth in loan volume from fintech lenders, which is expected to continue, and an increase in fintech lender-bank partnerships. Specifically, GAO found that of the fintech lenders surveyed, loan volume grew from $2.5 billion in 2013 to $17.7 billion in 2017. Some analysts project that fintech lending volume could reach between $90 billion and $122 billion by 2020. This growth presents a unique opportunity to expand access to financial services to communities that have historically been un- and underbanked. In a report, GAO also noted that most fintech lenders surveyed partnered with federally regulated banks to originate loans, and this partnership model is the most prevalent business model among fintech lenders in the United States. Finally, GAO found the biggest challenge faced by fintech lenders is compliance with varying state regulations. GAO recommended that regulators communicate with fintech lenders on the appropriate use of alternative data.[45]

Mr. Girouard also addressed concerns that the use of alternative data and AI in underwriting decisions may introduce bias or lead to disparate impact against protected classes of consumers. Mr. Girouard testified that concerns over fairness in algorithmic lending are "well founded," but further stated,

> [I]n Upstart's experience, the fair lending laws enacted in the 1970s and the substance of fair lending regulation enforcement—that is, monitoring and testing the impact on actual consumers who apply for loans—translates very well to the AI-driven world of today.[46]

Further, Upstart worked with the CFPB to "determine the proper way to measure bias," and developed automated tests to "provide reports on the impact of [their] credit decisions across underserved groups."[47] Through these tests, Upstart demonstrated that their algorithm did not have disparate negative impact on those classes of consumers. In fact, the opposite was true: "Upstart's model provides higher approval rates and lower interest rates for every traditionally underserved demographic."[48]

---

[43] *Id.*
[44] *Agencies Should Provide Clarification on Lenders' Use of Alternative Data*, GOVERNMENT ACCOUNTABILITY OFFICE, https://www.gao.gov/products/GAO-19-111.
[45] *Agencies Should Provide Clarification on Lenders' Use of Alternative Data*, GOVERNMENT ACCOUNTABILITY OFFICE, https://www.gao.gov/products/GAO-19-111.
[46] *Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit: Hearing Before the Task Force on Financial Technology of the H. Comm. on Financial Services, 116th Cong*., (July 25, 2019), *available at* https://docs.house.gov/meetings/BA/BA00/20190725/109867/HHRG-116-BA00-Wstate-GirouardD-20190725.pdf.
[47] *Id.*
[48] *Id.*

Congress should be encouraged by these outcomes and should continue to oversee new uses of AI to ensure that fairness concerns are adequately addressed. However, in light of the significant benefits of using alternative data in underwriting decisions, policymakers must ensure that they do not take steps that could hamper innovation which expands access to financial services and ultimately serves to advantage consumers, particularly those consumers that have been historically underserved.

ii. Algorithmic Bias

Beyond the use of AI in making lending decisions, critics have expressed concerns that the use of algorithms in financial services may include bias or lead to disparate outcomes.[49] After all, algorithms are written by humans, who may unintentionally include their conscious or unconscious biases in the programs they write.[50] These are concerns that Congress should, and does, take seriously.

In February 2020, the Task Force on Artificial Intelligence held a hearing to explore ways to reduce AI bias in financial services. Rayid Ghani, Distinguished Career Professor within the Machine Learning Department and the Heinz College of Information Systems and Public Policy at Carnegie Mellon University, testified for the Republicans.

The key issue in this space is algorithm explainability, or the idea that there should be transparency surrounding how an algorithm makes decisions. Professor Ghani testified that algorithms themselves are neither inherently biased or unbiased, rather, they work by analyzing past data and making generalizations about future outcomes.[51] Bias may enter the system when developers tell the system for which metric to optimize. However, "the AI developer can, in fact, tell the algorithm to balance replicating as many human decisions correctly as possible with ensuring fairness and equity across certain protected attributes of people that we care about."[52]

In January 2020, the White House Office of Science and Technology Policy (OSTP) released draft Guidance for Regulation of Artificial Intelligence Applications.[53] The principles therein reflect the

---

[49] *See, e.g.*, *The Week in Tech: Algorithmic Bias Is Bad. Uncovering It Is Good*, THE NEW YORK TIMES (Nov. 15, 2019), https://www.nytimes.com/2019/11/15/technology/algorithmic-ai-bias.html.
[50] *Id.*
[51] *Equitable Algorithms: Examining Ways to Reduce AI Bias in Financial Services: Hearing Before the Task Force on Artificial Intelligence of the H. Comm. on Financial Services, 116th Cong*., (Feb. 12, 2020), *available at* https://docs.house.gov/meetings/BA/BA00/20200212/110499/HHRG-116-BA00-Wstate-GhaniR-20200212-U1.pdf.
[52] *Id.*
[53] *Guidance for Regulation of Artificial Intelligence Applications*, THE WHITE HOUSE, https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf; *Artifical Intelligence for the American People*, THE WHITE HOUSE, https://www.whitehouse.gov/ai/executive-order-ai/.

need for explainability: "Best practices include transparently articulating the strengths, weaknesses, intended optimizations or outcomes, bias mitigation, and appropriate uses of the AI application's results."[54] The principles note that transparency should not follow a one size fits all equation, noting, "What constitutes appropriate disclosure and transparency is context-specific, depending on assessments of potential harms, the magnitude of those harms, the technical state of the art, and the potential benefits of the AI application."[55]

In addition to explainability, there must be an emphasis on testing an algorithm's outputs to ensure that those decisions are fair and accurate. Professor Ghani testified that a vital step in building equitable algorithms is validating the outcomes and continuous monitoring and evaluation of the AI system to ensure that it is achieving the desired outcomes with accuracy.[56]

OSTP's principles also note the importance of evaluating outcomes:

> When considering regulations or non-regulatory approaches related to AI applications, agencies should consider, in accordance with law, issues of fairness and non-discrimination with respect to outcomes and decisions produced by the AI application at issue, as well as whether the AI application at issue may reduce levels of unlawful, unfair, or otherwise unintended discrimination as compared to existing processes.[57]

It is important to note that the fact that an algorithm contains bias or leads to unintended outcomes does not mean that it is beyond repair or must be abandoned entirely. According to Professor Ghani, "it is possible to design a system that contains an algorithm that is not fair but coupled with the appropriate bias mitigation and intervention plan, can result in increasing equity in outcomes."[58] For example, he testified further that,

> In some recent preliminary work we did with Los Angeles City Attorney's office, we found that by careful consideration and analysis, we can mitigate the disparities that a potentially biased algorithm may create and coupled with a tailored

---

[54] *Guidance for Regulation of Artificial Intelligence Applications*, THE WHITE HOUSE, https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.
[55] *Id.*
[56] *Equitable Algorithms: Examining Ways to Reduce AI Bias in Financial Services: Hearing Before the Task Force on Artificial Intelligence of the H. Comm. on Financial Services, 116th Cong*., (Feb. 12, 2020), *available at* https://docs.house.gov/meetings/BA/BA00/20200212/110499/HHRG-116-BA00-Wstate-GhaniR-20200212-U1.pdf.
[57] *Guidance for Regulation of Artificial Intelligence Applications*, THE WHITE HOUSE, https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.
[58] *Equitable Algorithms: Examining Ways to Reduce AI Bias in Financial Services: Hearing Before the Task Force on Artificial Intelligence of the H. Comm. on Financial Services, 116th Cong*., (Feb. 12, 2020), *available at* https://docs.house.gov/meetings/BA/BA00/20200212/110499/HHRG-116-BA00-Wstate-GhaniR-20200212-U1.pdf.

> intervention strategy, the system has the potential to result in equitable criminal justice outcomes across racial groups.[59]

Importantly, the conversation cannot end with algorithms. Because the use of AI is often a compliment to human processes, oversight must also include how humans utilize AI outputs. As Professor Ghani testified,

> It is entirely possible to have a perfectly fair and equitable algorithm providing fair and equitable recommendations but the human decisions following them may be biased or the interventions allocated as a result of that human decision are not as effective for certain people as they are for others, resulting in inequity in outcomes.[60]

OSTP's principles also emphasize that regulation in this space be right-sized to avoid hampering innovation. Not only does this mean "carefully consider the full societal costs, benefits, and distributional effects before considering regulations," but also that any regulations should be designed to withstand the test of time:

> Rigid, design-based regulations that attempt to prescribe the technical specifications of AI applications will in most cases be impractical and ineffective, given the anticipated pace with which AI will evolve and the resulting need for agencies to react to new information and evidence.[61]

Congress must continue to examine the use of AI in financial services, using a data-driven approach to explore issues related to accuracy and consumer protection, including algorithmic bias. Congress should be encouraged by new applications of AI, but algorithmic decisions must be made with transparency to ensure that such biases are rooted out and mitigated.

iii. The Impact of AI on the Capital Markets

In December 2019, the task force on Artificial Intelligence held a hearing entitled "Robots on Wall Street: The Impact of AI on Capital Markets and Jobs in the Financial Services Industry" to explore the many ways that the use of AI and new surveillance technologies have modernized our capital markets.

---

[59] *Id.*
[60] *Equitable Algorithms: Examining Ways to Reduce AI Bias in Financial Services: Hearing Before the Task Force on Artificial Intelligence of the H. Comm. on Financial Services, 116th Cong*., (Feb. 12, 2020), *available at* https://docs.house.gov/meetings/BA/BA00/20200212/110499/HHRG-116-BA00-Wstate-GhaniR-20200212-U1.pdf.
[61] *Guidance for Regulation of Artificial Intelligence Applications*, THE WHITE HOUSE, https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.

Investing has changed dramatically over the past several decades. Most recently, the use of artificial intelligence has dramatically increased in investment strategies, particularly in the stock market. At least 35% of the $31 trillion in American public equities is held in computer-managed funds, and "90% of equity-futures trades and 80% of cash-equity trades are executed by algorithms without any human input."[62]

In particular, there has been a marked rise in so-called "robo-advisers," or investment advisers that are based on automated, algorithmic trading, rather than an active human manager. Reliance on algorithmic investing has several advantages, including increased efficiency and reduced cost. Investors may pay fees as low as 0.15% of the assets invested annually to a robo-adviser.[63]

The use of AI and algorithms can also enable stronger fraud detection and prevention strategies. As access to the markets increases, the number of participants rises. With the rise in participation, the volume of data that surveillance teams must review in order to assess threats to the market increases. Indeed, as Martina Rejsjo, Head of Nasdaq Market Surveillance for Nasdaq Stock Market, testified, "[t]his increase in players, the ability to deploy manipulative strategies with their own technology, and exponential increase in data quantities can act as the perfect ecosystem for market manipulators looking to hide amongst the noise."[64] The use of AI allows for more efficient and effective fraud prevention strategies by streamlining data review and reducing false-positive red flags. Those benefits also enable better compliance monitoring by financial institutions. According to Ms. Rejsjo, the use of AI and new technologies:

> [A]utomate[s] the detection, investigation and analysis of potentially abusive or disorderly trading—whether cross market, cross-asset, and multi-venue—to help improve the overall efficiency of the surveillance organization and reduce cost, even as market complexity and new regulations increase.[65]

AI is a tool to enable faster and more productive trading; humans have not been removed from the equation. There is widespread concern that automation and the use of artificial intelligence will eliminate jobs. For example, a 2019 report by Bank of America Merrill Lynch predicted that as many as 800 million jobs worldwide could be displaced by automation in the next 15 years.[66]

---

[62] *The stockmarket is now run by computers, algorithms and passive managers*, THE ECONOMIST (Oct. 5, 2019), https://www.economist.com/briefing/2019/10/05/the-stockmarket-is-now-run-by-computers-algorithms-and-passive-managers.

[63] *Automated investing that's tailored to you*, VANGUARD, https://investor.vanguard.com/advice/digital-advisor/.

[64] *Robots on Wall Street: The Impact of AI on Capital Markets and Jobs in the Financial Services Industry: Hearing Before the Task Force on Artificial Intelligence of the H. Comm. on Financial Services*, 116th Cong., (Dec. 6, 2019), *available at* https://docs.house.gov/meetings/BA/BA00/20191206/110292/HHRG-116-BA00-Wstate-RejsjoM-20191206.pdf.

[65] *Id.*

[66] *Automation could replace up to 800 million jobs by 2035: Bank of America Merrill Lynch*, YAHOO FINANCE (Nov. 12, 2019), https://finance.yahoo.com/news/automation-could-replace-up-to-800-million-jobs-by-2035-bank-of-america-merrill-lynch-171810646.html.

As Andrew McAfee and Erik Brynjolfsson describe in their book, *The Second Machine Age*, humans and computers have enjoyed a standard partnership in the digital age. That partnership entails machines handling routine processes, record keeping, and quantitative tasks so that humans can focus their time and attention on tasks involving creativity, judgment, and social interactions. And while the emergence of automation and robotics will transform life and labor in extraordinary ways, the reality is that many of the big breakthroughs that are seemingly within reach are actually difficult to achieve. Automated vehicles have been described as the "never-ending self-driving project."

Occupational churn, which is expected as automation has become more prevalent in the labor market, remains at historic lows in the United States. Concerns about job loss due to automation may be unfounded, as history shows that as new technologies serve as compliments to human employment, demand for goods and services often rises and leads to an increase in employment.[67] And in the financial services industry, where the ATM, for example, was introduced with widespread adoption and viewed as designed to replace human labor, the number of bank tellers actually rose between 2000 to 2010.[68] Congress should not fear new technologies, but should welcome the introduction of innovative products into our capital markets, which serves to reduce cost to investors and enable better decision making.

C. Protecting Consumer Financial Data in a Cloud Computing Age

Over the past decade, the financial services industry has undergone a massive transformation in terms of artificial intelligence, cloud computing, and machine learning—all of which rely on big data. As a result, the collection, use, and sharing of a massive trove of consumer financial data allows financial firms to provide substantial improvements in how financial services are delivered and consumed, but it also creates new areas of risk.

Especially in the realm of AI and machine learning that relies on personal information for big data analytics, financial institutions are adapting new approaches in order to follow the changing landscape of compliance.

That includes more robust measures in terms of risk management, cybersecurity, and the use of third-party technology providers. Cybersecurity has been of particular focus as financial markets and intuitions increasingly rely on the use of consumer financial data to perform their core functions. In 2016, the Office of Financial Research wrote in its Financial Stability Report to Congress that the vulnerabilities of financial firms in terms of cybersecurity could have systemic

---

[67] *What the story of ATMs and bank tellers reveals about the 'rise of the robots' and jobs*, AEI (June 6, 2016), https://www.aei.org/economics/what-atms-bank-tellers-rise-robots-and-jobs/.
[68] *Id.*

risk implications. Moreover, financial institutions have prioritized cybersecurity as their number one concern, spending "ten percent of their information technology budgets on cyber security or 0.3 percent of their total revenues."[69]

Unlike other industries, the nature and use of consumer data is strictly regulated in financial services because of the data involved. Consumer financial data includes some of the most personal of information for the consumer, including: credit card numbers, credit scores, savings, spending habits such as information about medical bills, tuition, and other sensitive expenditures, and other financial information. The centrality of this type of personal financial data in terms providing a more digital experience is also why the data itself is becoming so valuable in the financial services industry.

i. Existing Regulatory Framework

GLBA

Twenty years ago, the Gramm-Leach-Bliley Act (GLBA) was signed into law, requiring financial institutions to explain how they share and protect consumers' private information. Specifically, GLBA prohibits financial institutions from sharing nonpublic information with nonaffiliated third parties, unless the financial institution provides consumers with notice and an opportunity to "opt-out." Notice includes categories of the type of data collected, the types of third parties with whom the financial institution shares the data, and the policies and procedures that are in place to protect the confidentiality and security of the data.[70]

The primary data protections under GLBA are provided in what is commonly referred to as the "Safeguards Rule." The Safeguards Rule requires that financial institutions must maintain "administrative, technical, and physical safeguards" to "ensure the security and confidentiality" of customers' data, and to protect against any "anticipated threats or hazards . . . [or] unauthorized access" to such information.[71]

In addition to GLBA, the financial services sector must comply, where applicable, with the Fair Credit Reporting Act (FCRA), which governs the use of data for consumer credit determinations. The FCRA provides the rules regarding the collection and use of financial information by credit reporting agencies (CRAs), as well as third parties that furnish the information to the CRAs. Specifically, the FCRA requires that the data provided and used by the CRAs is accurate for consumer credit reports. Additionally, the FCRA limits the use of consumer reports for a

[69] *Financial firms devote 10% of IT budgets to cybersecurity: Survey*, BUSINESS INSURANCE (May 3, 2019), https://www.businessinsurance.com/article/00010101/NEWS06/912328259/Financial-firms-devote-10-of-IT-budgets-to-cybersecurity-Survey.
[70] 12 C.F.R. § 1016.6(a).
[71] 15 U.S.C. § 6801(a); 16 C.F.R. § 314.3.

"permissible purpose," including: employment decisions, insurance underwriting, and "legitimate business need" in connection with a business transaction involving the consumer, such as a mortgage or other consumer loan.[72]

GDPR and CCPA

More recently, the European Union adopted an overarching data-protection law called the General Data Protection Regulation (GDPR). Implemented in 2018, GDPR impacts the processing of personal data for organizations that have an "establishment" in the EU. While "establishment" is not defined, effectively GDPR applies to any organization that has "any real and effective activity" on the Internet.[73] It sets out the following seven key principles for the processing of personal data: (1) lawfulness, fairness, and transparency; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; and (7) accountability.[74] Based on these principles, an Internet page now provides a notice on its privacy and cookie policy, requiring user consent to proceed on the webpage.

While the United States has not adopted GDPR, the State of California adopted its own version of GDPR, called the California Consumer Privacy Act (CCPA). While the CCPA exempts certain types of personal financial information under the FCRA and GLBA from its reach,[75] it is important to note that the exemption applies to the type of data, not the type of companies that handle the data. Thus, the CCPA applies to financial institutions as it relates to "personal information" that is not covered under the FCRA and GLBA. The type of personal may include, for example, the IP address that is collected by the financial institution's website or data provided by the financial institution to an affiliate whenever a user visits their website.[76]

The CCPA became effective on January 1, 2020 and, because there is no overarching federal data privacy law, the CCPA has been treated as the de facto regulation for data privacy in the United States. At the very least, the CCPA has established a new floor for American data privacy laws in the future.

Under GDPR and CCPA, banks are under new obligations in terms of how consumer financial data is handled. For example, financial institutions now have to report data breaches to authorities within 72 hours of their discovery. Additionally, financial institutions now have to provide

---

[72] 15 U.S.C. § 1681b(a).
[73] GDPR, art. 3(1).
[74] GDPR, art. 5.
[75] *Assembly Bill No. 1355*, CALIFORNIA LEGISLATIVE INFORMATION, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1355.
[76] *Are Banks and Other Lenders Subject to the CCPA?*, CARLTON FIELDS (Aug. 29, 2019), https://www.carltonfields.com/insights/publications/2019/are-banks-and-other-lenders-subject-to-the-ccpa.

customers with full access to the data being collected, and the financial institution will have to respond when a consumer requests the deletion of their data.

Until a national standard is adopted in the United States, questions will remain about what protections consumers should, and do, enjoy with regards to their financial data, and what obligations are imposed on those entities that collect, use, and share that data. Currently, both consumers and financial services providers face some uncertainty around issues like consent, data ownership, and the potential for additional regulations by financial regulators. This uncertainty is compounded by the promulgation of state laws, which impose varying, and sometimes conflicting, rights and obligations. As the use of consumer financial data becomes ever more ubiquitous in the financial services industry, and vital to innovation across the multiple industries, it is important that Congress act to enact appropriate safeguards for consumers.

ii. Dodd Frank 1033

As private sector innovation expands the frontiers of what is possible in financial services, it is critical that consumers remain empowered in the management of their financial lives. Policymakers in financial services have long focused on facilitating a baseline of fair dealing and informed consent when consumers interact with financial institutions. Now, with the emergence of new technologies and business models, Congress must also take on the task of developing a rational, pro-competition approach to putting consumers in the driver's seat when it comes to their nonpublic personal financial information.

In 2010, Congress authorized the Consumer Financial Protection Bureau, under section 1033 of the Dodd-Frank Act, to enable consumers to have access to and the ability to leverage their own personal financial data.[77] Section 1033 authorizes the CFPB to promulgate rules directing consumer financial services providers to share with a consumer the information in the control or possession of the provider concerning the consumer financial product or service that the consumer obtained from the provider.

Since enactment of section 1033, the extent to which financial institutions, data aggregators, and fintechs are using consumer-authorized access to provide new products and services to millions of American consumers has only grown in scope and scale. Meanwhile, the CFPB has yet to establish clear rules of the road. In 2016, the Bureau issued a request for information concerning section 1033.[78] In 2017 it followed up with a report of stakeholder insights and a set of consumer

[77] *See* § 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111–203 (Jul. 21, 2010) (12 USC 5533).
[78] See 81 FR 83806 (Nov. 22, 2016).

protection principles "intended to reiterate the importance of consumer interests to all stakeholders in the developing market for services based on the consumer-authorized use of financial data."[79] The principles cover topics such as: access; data scope and usability; control and informed consent; authorizing payments; security; access transparency; accuracy; ability to dispute and resolve unauthorized access; and efficient and effective accountability mechanisms. The principles themselves are not enforceable, however, and the preamble to the list specifically disclaims any legal effect.

In February 2020, the CFPB invited a wide range of stakeholders to a symposium regarding consumer access to financial records.[80] Featuring a wide array of stakeholders—from banks to fintechs to consumer advocates—the symposium produced a fulsome dialogue about the questions posed by section 1033, setting the groundwork for the Bureau to take tangible steps towards developing a regulatory framework.

In October 2020, the CFPB published an Advanced Notice of Proposed Rulemaking (ANPR) to implement section 1033.[81] Through this initial step, the CPFB sought comments and information on the costs and benefits of consumer data access; competitive incentives; standard-setting; access scope; consumer control and privacy; and data security and accuracy. The CFPB has promised a transparent and deliberate rulemaking process. This is key to fostering consumer trust and producing a rational regulatory regime that does not destroy the vital innovation and competition coming from the private sector. The comment period for the ANPR closed on February 4, 2021.

iii. Cloud computing

Technology-enabled financial services companies are increasingly relying on cloud computing for their data storage and processing needs. The core characteristics of cloud computing are on-demand, self-service, broad network access, resource pooling, rapid elasticity, and measured

[79] *Consumer-authorized financial data sharing and aggregation: Stakeholder insights that inform the Consumer Protection Principles*, CFPB (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_dataaggregation_stakeholder-insights.pdf; *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, CFPB Oct. 18 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.
[80] *CFPB Symposium: Consumer Access to Financial Records*, CFPB (Feb. 26, 2020), https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-consumer-access-financial-records/.
[81] *CFPB Symposium: Consumer Access to Financial Records*, CFPB (Feb. 26, 2020), https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-advance-notice-proposed-rulemaking-consumer-access-financial-records/; *see also Bureau Symposium: Consumer Access to Financial Records: A summary of the proceedings*, CFPB (Jul. 2020), https://files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financialrecords_report.pdf.

service.[82] Cloud services offer many advantages to financial institutions, including increased speed and efficiency of data processing, lower costs, and better compliance with relevant regulations.

In October 2019, the Task Force on Artificial Intelligence held a hearing entitled "AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers." Paul Benda, Senior Vice President of Risk Cybersecurity Policy for the American Bankers Association testified to the Committee. Mr. Benda's testimony outlined the benefits and risk of utilizing cloud services. He also spoke to the need for greater regulatory certainty as the use of cloud computing continues to grow throughout the financial services industry.

While most banks have adopted cloud computing for non-core operations, the financial services industry has been slow to adopt cloud computing for core operations due to regulatory uncertainty.[83] Specifically, there remains uncertainty around data privacy and security, including the handling of breaches, service disruptions, and data recoverability. However, experts expect many major banks to rely heavily on cloud services within several years.

The use of cloud services offers several benefits both to financial institutions and consumers. Cloud services enable financial institutions and other enterprises to manage computing resources through a utility-like model, scaling use up or down based on demand. This allows financial institutions and others to pay only for the resources they actually need and use at a given time. This reduces both the cost of technology infrastructure and the cost of over-provisioning. Because cloud computing lowers costs, it allows smaller financial institutions to compete with larger financial institutions. This in turn helps expand access to financial services to unbanked and underbanked consumers.

The scalability and flexibility provided by cloud computing can also enable companies to operate with more efficiency and agility. Companies can develop and test new products and services through cloud services with more speed than on traditional platforms.

Further, because cloud services are able to process large data sets more quickly, cloud computing can also provide additional security compared to traditional platforms, particularly for smaller institutions that lack the resources available to larger institutions. Cloud services can employ automated mechanisms that can detect fraud and security issues more rapidly than traditional

---

[82] Peter Mell and Timothy Grance, The NIST Definition of Cloud Computing, 2 (NIST Special Publication 800-145, Sept. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[83] *Regulatory Ambiguity Is Slowing Bank Adoption of Cloud Services*, AMERICAN BANKER (Aug. 30, 2016), https://www.americanbanker.com/opinion/regulatory-ambiguity-is-slowing-bank-adoption-of-cloud-services;*AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers: Hearing Before the Task Force on Artificial Intelligence of the H. Comm. on Financial Services*, 116th Cong., (Oct. 18, 2019), *available at* https://docs.house.gov/meetings/BA/BA00/20191018/110094/HHRG-116-BA00-Wstate-BendaP-20191018.pdf.

platforms. This, in turn, can enable financial institutions to mitigate risk and achieve better security.

While the use of cloud services comes with many advantages, financial institutions that choose to use cloud services face several risks, both technical and operational. Technical risks include privacy considerations, particularly the risk that because multiple customers of a cloud provider share the same physical infrastructure, a customer could inadvertently expose their data to others. According to Mr. Benda's testimony to the Committee,

> Utilizing the cloud does not necessarily increase the risks a financial institution may face, but simply changes the nature of the risk. A financial institution is in the business of storing sensitive financial data. This data must be protected regardless of where it may be stored, whether hosted on premise or in a public or private cloud. But while data is stored in physical infrastructure that is managed by a third party, such as the cloud, access and other controls must be tailored to the specific cloud implementation. For institutions that conduct appropriate due diligence on their [cloud service provider] and take a deliberate approach to securing their cloud environment, there may be no difference in risk from an on-premise environment and a cloud-based environment. In many ways, in a cloud environment, overall risks may be reduced due to the operational resilience capabilities and scalable architecture that a [cloud service provider] can provide in the event of some type of capability failure.[84]

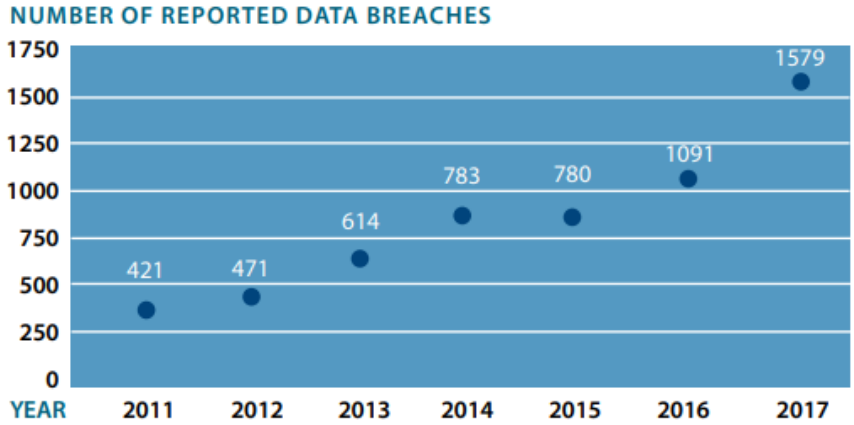
Critics have also expressed concerns that use of cloud services by financial institutions could open banks to higher risk of cyberattacks. In July 2019, a former engineer at Amazon Web Services (AWS) gained access to a financial institution's server and exposed the personally identifiable information of more than 100 million customers.[85] Following the breach, the Ranking Member sent a letter to Vice Chair for Supervision at the Federal Reserve, Randal Quarles, requesting any information during their examination process, including a detailed explanation of the Fed's examination procedures for third party service providers.[86]

Cyber-attacks pose one of, if not the, greatest threats to the financial system. Late last year the Harvard Business Review ranked cyber-attacks as the biggest threat facing the business world

---

[84] *AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers: Hearing Before the Task Force on Artificial Intelligence of the H. Comm. on Financial Services*, 116th Cong., (Oct. 18, 2019), *available at* https://docs.house.gov/meetings/BA/BA00/20191018/110094/HHRG-116-BA00-Wstate-BendaP-20191018.pdf.
[85] *Capital One Data Breach Compromises Data of Over 100 Million*, THE NEW YORK TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.
[86] *Ranking Member McHenry Presses Fed for Capital One Data Security Breach Details*, COMMITTEE ON FINANCIAL SERVICES, (Aug. 5, 2019), https://republicans-financialservices.house.gov/news/documentsingle.aspx?DocumentID=407394.

today — ahead of terrorism, asset bubbles, and other risks. According to the Identity Theft Resource Center, the number of reported data breaches has increased from 421 in 2011 to 1,579 in 2017. 765 million people were victims of a data security breach in the second quarter of 2018 alone. The following chart shows the increased number of breaches since 2011:



These breaches have exposed the PII of hundreds of millions of people globally. Not only do such breaches threaten individuals' privacy, identity theft results in billions of dollars lost annually. In 2017, $16.8 billion was lost due to identity fraud in the United States alone.[87] The following chart provides a summary of the many costs associated with identity fraud:

[87] *Better Identity in America: A Blueprint for Policy Makers*, THE BETTER IDENTIFY COALITION, https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/5d419caa5001d70001614b8f/1564581036670/Better_Identity_Coalition%2BBlueprint%2B-%2BJuly%2B2018.pdf.

Protection against cyber-attacks is also costly: estimated information security costs for U.S. financial institutions are expected to total $68 billion in spending between 2016 and 2020.[88]

Financial services firms fall victim to cybersecurity attacks approximately 300 times more frequently than other businesses.[89] This is, in part, because cyber-criminals seek not only financial gains but also to disrupt critical infrastructure. Increased risk for financial firms can also be attributed to the many partnerships on which they rely, including cloud service providers. The interconnected nature of banks and third-party vendors, such as processors, information technology services, and loan review and servicing raise the exposure of financial institutions to cyber-attacks.

---

[88] *Forces Shaping The Cyber Threat Landscape For Financial Institutions*, SWIFT INSTITUTE, https://csis-prod.s3.amazonaws.com/s3fs-public/171006_Cyber_Threat_Landscape%20_Carter.pdf?UWqJEbDm.dBKSLEIFTyYs1IxJaExh9Y7.

[89] *The Cost Of A Cybersecurity Breach For Financial Institutions*, ITSP (Mar. 20, 2018), https://www.itspmagazine.com/from-the-newsroom/the-cost-of-a-cybersecurity-breach-for-financial-institutions.

In its 2018 annual report, the Financial Stability Oversight Council (FSOC) cited cybersecurity as a perennial key financial stability vulnerability. FSOC highlighted a cyber-attack could result in the disruption of a key financial service or utility, the loss of confidence in the system, and the compromising or disruption of critical data upon which the financial firms and systems rely.[90] As the financial system increases its reliance on information technology, the risk increases that a cybersecurity event in the industry will have severe negative consequences. Thus, ensuring that the U.S. financial system is resilient enough to deal with a possible cyber-attack, is, and will continue to be a key concern for FSOC.

Banks that choose to use cloud computing are subject to several regulations that address how financial institutions must manage risk. In particular, Gramm-Leach-Bliley Act (GLBA) imposes requirements surrounding data privacy, while the Bank Service Company Act (BSCA) imposes requirements surrounding the use of third-party vendors by financial institutions.

Under GLBA, financial institutions are prohibited from sharing nonpublic personal information with unaffiliated third parties unless the consumers are provided notice and an opportunity to opt-out.[91] The notice must include the type of data collected, the categories of third parties with whom the financial institution shares data, and the polices to protect the confidentiality and security of the nonpublic personal information. Furthermore, the GLBA tasks financial services regulators with establishing administrative, technical, and physical safeguards that financial institutions must follow to protect customer information, regardless of whether customer information is stored by the financial institution itself, or with a cloud service provider.

With respect to the BSCA, depository institutions are required to notify the regulators of their relationships with service providers.[92] Historically, the type of relationship covered by BSCA would include administrative third-party functions such as check and deposit sorting, bookkeeping, and other clerical functions. However, the agencies have interpreted BSCA to include third parties engaged in data processing, online and mobile banking.

In addition, financial institutions are subject to oversight by the federal banking agencies. The Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), and National Credit Union Administration (NCUA) all examine institutions for data security standards and third-party vendor management. Financial institutions, such as [], that fall under the jurisdiction of the Federal Trade Commission (FTC) must also adhere to the FTC Safeguards Rule which outlines further requirements to keep consumer information secure.

---

[90] 2018 FSOC Annual Report, U.S. DEPARTMENT OF TREASURY, https://home.treasury.gov/system/files/261/FSOC2018AnnualReport.pdf.
[91] *See* 15 USC 6801, et seq.
[92] *See* 12 USC 1867(c)(2).

In addition to laws and regulations, the financial services regulators have published specific guidance about the use of cloud computing by regulated entities. The Federal Financial Institutions Examination Council (FFIEC) is focused on promoting uniformity and consistency in the supervision of financial institutions and has developed the Cybersecurity Assessment Tool to help institutions identify risks and promote cybersecurity preparedness. In addition, the FFIEC Information Technology Examination Handbook provides detailed guidance on regulatory expectations surrounding outsourced technology services. In 2012, the FFEIC published guidance entitled "Outsourced Cloud Computing."[93] Specifically, it provides that financial institutions ensure that cloud service providers meet the institutions' needs with respect to cost, quality of service, regulatory compliance, and risk management.

In April 2020, the FFIEC published additional guidance on Risk Management for Cloud Computing Services.[94] The guidance did not include new regulatory expectations but highlighted best practices and provided a list of resources to assist financial institutions in compliance when partnering with third party cloud service providers.

In 2013, the OCC issued guidance on third party risk management, known as OCC Bulletin 2013-29.[95] The guidance includes recommendations for banks to identify third-party relationships that involve critical activities and ensure the bank adopts risk management processes commensurate with the level of risk and complexity of those relationships.

As Mr. Benda testified to the Committee,

> The GLBA mandates that financial institutions protect their customer data. While typical cloud implementations follow a shared responsibility model for data security in which the CSPs have certain responsibilities related to the security of, for example, the physical infrastructure of the relevant cloud, the utilization, deployment, security and administration of such resources made available by the CSP, however, are ultimately the responsibility of the financial institution using the cloud.
>
> ....

---

[93] *Federal Financial Regulators Release Statement on Outsourced Cloud Computing*, FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (July 10, 2012), https://www.ffiec.gov/press/pr071012.htm; *Outsourced Cloud Computing*, FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf.
[94] *FFIEC Issues Statement on Risk Management for Cloud Computing Services*, FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, https://www.ffiec.gov/press/pr043020.htm.
[95] *Third-Party Relationships: Risk Management Guidance*, OFFICE OF THE COMPTROLLER OF THE CURRENCY, (Oct. 30, 2013), https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

> While many CSPs currently publish attestations to the audits their services have undergone, for financial institutions increased transparency into the business continuity, security incident and breach response, and testing programs would help them comply with their regulatory requirements. Additionally, in the shared services model there are some CSPs that provide different options to customers regarding who manages some security controls. Additional transparency into these options and how the control environment is executed would help financial institutions manage both their risk and those of their third parties who utilize the cloud.[96]

As more financial institutions begin to rely on cloud computing to offer their customers the numerous advantages of those services, there may be a need for greater regulatory certainty with regards to the oversight of third-party cloud service providers. Regulatory certainty will help ensure that consumers' financial data is adequately protected.

Further, there is no federal standard for data security for non-financial institutions that handle consumer data. A uniform standard would allow financial institutions to shift resources from compliance to real data protection.

iv. Digital ID

Establishing a digital identity is necessary to bank online, buy and sell products, access health records, and even pay taxes. Historically, digital identity verification relies on personally identifiable information (PII). PII includes social security number, date of birth, and home address. However, such sensitive information is vulnerable to theft. Both private industry and the government have started to find ways to balance privacy and security, while enabling the American people to conduct more transactions online.

High-profile breaches, particularly at companies the American public should be able to trust to keep their information safe, demonstrates that our reliance on outdated models like Social Security numbers puts American families at risk.

In September 2019, the Task Force on Artificial Intelligence held a hearing entitled "The Future of Identity in Financial Services: Threats, Challenges, and Opportunities." Witnesses testified as to the pitfalls of our current identity verification system. Andre Boysen, Chief Identity Officer for SecureKey, outlined the possibility of a privacy-based digital identity verification system created on blockchain technology. The blockchain uses a "triple blind" privacy protocol. This allows users

---

[96] *AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers: Hearing Before the Task Force on Artificial Intelligence of the H. Comm. on Financial Services*, 116th Cong., (Oct. 18, 2019), *available at* https://docs.house.gov/meetings/BA/BA00/20191018/110094/HHRG-116-BA00-Wstate-BendaP-20191018.pdf.

to choose to share information within a network of organizations that they already trust. In turn, the participating organizations that use the network do not have access or visibility to all of the data of that particular consumer. Instead, the transaction is with a "trusted" source. According to Boysen:

> This scenario is not part of the distant future. All of the pieces are already in place to allow the providers of data to enable a system that has authoritative information, that provides receivers of information with confidence in the transaction, and for the citizen to fully trust the system as they control their own data in a privacy-enhanced way. This type of arrangement is the cutting edge and is happening now in Canada, with our Verified.Me digital identity verification network.[97]

The United States is woefully behind. Jeremy Grant, Coordinator for the Better Identity Coalition and witness for the Majority, explained that while individuals have greater ability to access their information online through authentication tools other than passwords, verifying an individual's identity during initial account creation is growing more difficult. Grant also testified that the standards adopted by Fast Identities Online Alliance (FIDO) mark "the most significant development in the authentication marketplace in the last 20 years."

Relying on usernames and passwords alone to verify identity is not sufficient. According to Mr. Grant, "81% of hacking attacks were executed by taking advantage of weak or stolen passwords."[98] There are various ways to verify one's identity online. One common method is Knowledge-Based Verification (KBV). KBV requires individuals to respond to a series of questions that, presumably, could be answered correctly only by that individual. However, critics have questioned the effectiveness of KBV, as well as identified serious vulnerabilities.

Further, as the frequency of data breaches increases, KBV data sets can be stolen and aggregated. This allows a fuller picture of an individual's identity to be formed, thereby facilitating further identity theft. One example of such aggregation was the 2015 hack of the IRS's "Get transcript" application, through which the sensitive tax information of more than 700,000 Americans was exposed.

In the 116th Congress, Ranking Member McHenry introduced legislation that would prohibit consumer reporting agencies from using the full Social Security Number (SSNs) for verifying consumers. It is estimated that up to 80% of all consumer SSNs have been stolen as a result of

---

[97] *The Future of Identity in Financial Services: Threats, Challenges, and Opportunities: Hearing Before the Task Force on Artificial Intelligence of the H. Comm. on Financial Services*, 116th Cong., (Sept. 12, 2019), *available at https://docs.house.gov/meetings/BA/BA00/20190912/109912/HHRG-116-BA00-Wstate-BoysenA-20190912.pdf.*
[98] *The Future of Identity in Financial Services: Threats, Challenges, and Opportunities: Hearing Before the Task Force on Artificial Intelligence of the H. Comm. on Financial Services*, 116th Cong., (Sept. 12, 2019), *available at* https://docs.house.gov/meetings/BA/BA00/20190912/109912/HHRG-116-BA00-Wstate-GrantJ-20190912.pdf.

cyber breaches at local, state, and federal government entities and companies across various industries.[99] Additionally, Ranking Member McHenry sent a letter to Vice Chair for Supervision at the Federal Reserve, Randal Quarles, subsequent to the July 2019 breach of a financial institution requesting any suspicious information during their examination process, including a detailed explanation of the Fed's examination procedures for third party service providers.

It is critical that the mechanisms by which Americans are identified are modernized, particularly for the purposes of verifying personal information with financial institutions. The current system is not protecting consumers' personally identifiable information. Additionally, consumers should have a more streamlined experience when going through the identification verification process to avoid having to remember old passwords or security questions. Finally, as this process of identity verification becomes more digital, policymakers must ensure that safeguards are in place to preserve the privacy of American citizens.

IV. Conclusion

This report marks the culmination of the Task Forces on Financial Technology and Artificial Intelligence, but our work in this space is not done. There are many topics the Committee did not explore in depth in the 116th Congress, including the use of regulatory technology and AI to streamline agencies' notice and comment process, the need for federal data privacy legislation, the future of decentralized finance, non-fungible tokens, and insurance tech (InsureTech).

Committee Republicans remain committed to exploring the promising uses of Financial Technology and Artificial Intelligence, and the numerous benefits they offer to consumers and financial services providers alike.

Recommendations

Congress's intent in the financial technology space must be to promote greater financial inclusion and nurture innovation. Policy makers can achieve these goals by pursuing three broad policy objectives:

America Must Remain on the Forefront of Global Payments: As our financial markets become increasingly globalized in nature, America must lead in global payments. As our peers develop their own digital currencies and real-time payments systems that allow consumers to send and receive funds instantly, it is incumbent upon the United States to maintain its status as a global

[99] *Theft Of Social Security Numbers Is Broader Than You Might Think*, NPR (June 15, 2015), https://www.npr.org/sections/alltechconsidered/2015/06/15/414618292/theft-of-social-security-numbers-is-broader-than-you-might-think.

leader in payments and to maintain the strength of the dollar both here and abroad. Action is needed in the following areas:

- Congress must continue oversight of the Federal Reserve's FedNow program to ensure that private sector innovation encouraged, rather than stifled, and that FedNow is fully interoperable with the private-sector instant payment service to accomplish the goal of nationwide reach for instant payments.
- Congress must clarify how digital assets are categorized and regulated in order to provide consumers with the confidence to make smart investment decisions, to provide innovators with the regulatory certainty needed to continue building innovative products, and to ensure that America remains a competitor in global markets.

Congress Must Foster Automation Which Leads to Better Decision Making: The use of AI in financial services holds great promise in combating fraud, streamlining compliance, making more inclusive underwriting decisions, and promoting financial inclusion.

- Congress must continue to examine the use of AI in financial services, using a data-driven approach to explore issues related to accuracy and consumer protection, including algorithmic bias.
- Congress must support the development of AI in the United States to ensure that America remains competitive in the global AI race.

Congress Must Keep Up with Technology to Better Protect Consumers: As the use of financial technology continues to evolve and proliferate, policymakers must create an infrastructure to support financial innovation and provide greater regulatory flexibility. We must act to modernize our regulations to meet the needs of the modern consumer and the modern financial services industry. Action is needed in the following areas:

- Congress must update our regulatory framework, including BSA/AML regulations, to ensure that bad actors cannot exploit outdated laws by using new technologies, such as virtual currencies.
- Congress must examine how technology is being used to aggregate consumer financial data and modernize statutes such as the Graham-Leach-Bliley Act to ensure consumers can control how their data is used.
- Congress must encourage the private and public sector to modernize the process of identity verification in America.