MAXINE WATERS, CA
CHAIRWOMAN

United States House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

PATRICK MCHENRY, NC
RANKING MEMBER

June 21, 2019

Memorandum

To: Members, Committee on Financial Services

From: FSC Majority Staff

Subject: June 26, 2019, "Perspectives on Artificial Intelligence: Where We Are and the Next Frontier in Financial Services,"

The Task Force on Artificial Intelligence of the House Financial Services Committee will hold a hearing entitled, "Perspectives on Artificial Intelligence: Where We Are and the Next Frontier in Financial Services," on June 26, 2019 at 10:00 a.m. in Room 2128 of the Rayburn House Office Building. This single-panel hearing will have the following witnesses:

- **Dr. Nicol Turner-Lee,** Fellow, Governance Studies, Center for Technology Innovation, Brookings Institution
- **Dr. Bonnie Buchanan**, Head of School of Finance and Accounting and Professor of Finance, Surrey Business School, University of Surrey
- **Dr. Douglas Merrill**, Founder and CEO, ZestFinance
- **Mr. R. Jesse McWaters,** Financial Innovation Lead, World Economic Forum

Overview

The use of artificial intelligence (AI) in the financial industry has grown exponentially in recent years, with financials products and tools such as consumer loans, credit reports, compliance review, trading, and banking services being increasingly automated. The development of AI has the potential to create computer programs that exceed human capabilities in certain tasks, such as quantitatively analyzing data sets and predicting outcomes based on those analyses. However, many of the AI services and technologies are being implemented with minimal regulation or oversight, and with little research into the societal and economic implications of increasing usage of AI in the financial industry. This memo will discuss methods to assess the social implications of AI in our financial sector; the data privacy and civil liberty implications of AI; the likelihood of exacerbating discrimination and disparate impact for low-income and minority consumers in a financial sector utilizing AI; and the regulatory and legislative proposals on how to address regulatory weaknesses or gaps regarding AI to better protect consumers.[1]

While there is no single, commonly agreed upon definition, AI can broadly be described as computerized systems that work and react in ways thought to require intelligence, such as solving complex problems in real-world situations.[2] In practice, AI is often described as a field that encompasses a range of methodologies and application areas, such as machine learning (ML), natural language processing

[1] This memo was prepared with the assistance of David W. Perkins, Laurie A. Harris, Rena S. Miller, and Eva Su from the Congressional Research Service (CRS). This memo is not exhaustive of all issues relating to AI in the financial sector. For more information from CRS, see https://www.crs.gov/Reports/IF10608 and https://www.crs.gov/Reports/IF10513.
[2] Office of Science and Technology Policy, Preparing for the Future of Artificial Intelligence, October 2016, p.6.

(NLP), and robotics. To date, definitions of AI put forth in legislation[3] have incorporated, to varying extents, a commonly cited framework of four possible goals that AI systems may pursue: systems that think like humans (e.g., neural networks), act like humans (e.g., natural language processing), think rationally (e.g., logic solvers), or act rationally (e.g., intelligent software agents embodied in robots).[4] However, AI research and applications do not necessarily fall neatly within any one of these four categories.

Types of Artificial Intelligence

Though more nuanced AI-related terms are also described in slightly different ways, the following frequently used terms include some broad definitions:

1. AI Systems are often described as either “narrow AI” (technologies tailored to narrowly defined tasks) or “general AI” (systems that demonstrate intelligent behavior across a range of cognitive tasks).
2. Machine learning~~,~~ (ML) examines how to develop computer programs that automatically improve their performance at some task through experience without relying on explicit rules-based programming to do so.[5] One of the goals of ML is to teach algorithms to successfully interpret data that have not been previously encountered. ML is one of the most common AI techniques in use today.
3. Neural networks, a particular type of machine learning loosely modeled after the human brain, consist of thousands or millions of processing nodes often organized into input and output layers. The strength of the connections among nodes and layers are repeatedly transformed, so that input data can be later used by the output layer.[6]
4. Natural language processing is the automatic manipulation of natural language (speech and text) by software.[7]

The Future of Artificial Intelligence in Financial Services

Many of the benefits, challenges, and potential societal implications that AI technologies present broadly are of potential concern for financial service applications. Some of these include data access, management, and bias (e.g., the potential of historical biases in datasets to be perpetuated or amplified in AI systems); opacity and explainability of the systems (e.g., the ability, or inability, of an AI system to explain decisions and actions to human users); and the availability of AI expertise, training, and education programs.

Algorithmic Bias leading to Disparate Impact and Discrimination in Artificial Intelligence

Proponents of AI and fintech lending argue that, because financial technologies increasingly use new data sources and new more sophisticated methods of analysis, the technologies may expand the availability of credit and services to individuals and small businesses in a fair, safe, and less costly way.[8] If the programs doing the analysis are able to learn from loan performance and automatically develop better assessment techniques over time, those efficiencies could be even greater. Similarly, if financial

[3] Section 238 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232) included the first definition of AI in federal law, specified for the purposes of the section.

[4] Stuart Russell, Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed. (Upper Saddle River, NJ: Prentice Hall, 2010), pp. 1-5.

[5] Adapted from Erik Brynjolfsson, Tom Mitchell, and Daniel Rock, "What Can Machines Learn, and What Does It Mean for Occupations and the Economy?," *AEA Papers and Proceedings*, vol. 108 (May 1, 2018), pp. 43-47, available at https://ssrn.com/abstract=3224100.

[6] Luke Dormehl, *What is an artificial neural network? Here’s everything you need to know*, Digital Trends, at https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/

[7] Ronan Collobert et al, *Natural Language Processing (Almost) from Scratch*¸ Journal of Machine Learning Research 12 (2011) 2493-2537, p. 2493, at http://www.jmlr.org/papers/volume12/collobert11a/collobert11a.pdf.

[8] Letter from John H. Henson, Head of Compliance, Lending Tree Inc., to U. S. Department of the Treasury, September 30, 2015, at https://www.regulations.gov/document?D=TREAS-DO-2015-0007-0037.

institutions can adapt more detailed methods of identity verification, then underbanked populaces have a greater opportunity to fulfill know-your-customer compliance requirements to gain access to banking services. For example, the abundance of data now available to the lenders about prospective borrowers—either publicly or accessed with the permission of the borrower—means lenders can incorporate additional information into credit risk assessments.[9] Potentially, more data about a borrower could allow a lender to make an accurate assessment of—and thus extend credit to—prospective borrowers for whom traditional information is lacking (e.g., people with thin credit histories) or insufficient to make a determination about creditworthiness (e.g., small businesses).[10]

However, consumer advocates argue that AI algorithms created by fintech lenders with a relative lack of federal regulatory supervision could inadvertently violate consumer protection regulations. If these lenders start to utilize programs that learn and change their own underwriting algorithms, the lenders using those programs will arguably have even less control over the loan decision outcomes and less understanding of why the program is making lending decisions. This raises concerns about how these lenders would be able to comply with certain consumer protection regulations.[11] For example, when lenders deny a loan application they generally must send a notice to the applicant explaining the reason for the denial, called an adverse action notice. Concerns exist around how well lenders will understand and thus be able to explain the reasons for a loan denial to a consumer when AI technology makes this decision based off aggregates of data. This may particularly be the case with lenders potential use of alternative data or web-scraping tools to collect data about prospective borrowers.[12] Also, certain studies suggest that algorithmic underwriting can result in discriminatory outcomes.[13] These results suggest that AI could lead to biased lending decisions without lender oversight and if true, it would mean regulators may want to take steps to ensure algorithms used for compliance or predictive purposes are not subject to such bias.

A key question then is to what extent should humans be able to override decisions on regulatory compliance matters that are made by AI. Allowing for human override could possibly protect against so-called "training bias" in the AI itself or other problems with a particular AI program. However, it could also create a way for humans to short-circuit the usefulness of an AI-based compliance program that is meant to automatically report problems to regulators without human interference.

The "Black Box" Problem in Artificial Intelligence

The emergence of ML and other forms of AI in financial services has raised several policy concerns. AI and ML decision-making are sometimes described as a "black box," wherein it is not clear to the developers of the algorithm or the institution using it why the algorithm made particular decisions.[14] The complexity of some AI techniques, particularly ML algorithms, makes them difficult, if not impossible, to thoroughly audit, in part because these programs update themselves over time based on

[9] For example, some fintech lenders use rent and utility payment histories, cash flow statements, and educational information such as university attended and major of degree earned. See U.S. Government Accountability Office, *Financial Technology: Agencies Should Provide Clarification on Lenders' Use of Alternative Data*, GAO-19-111, December 2018, pp. 33-38, https://www.gao.gov/assets/700/696149.pdf.

[10] *Id.* at 19-23.

[11] David Stein, "AI in Lending: Key Challenges and Practical Considerations," *Law 360*, August 9, 2018, at https://www.law360.com/articles/1071151/ai-in-lending-key-challenges-and-practical-considerations.

[12] JetRuby Agency, *What is Web Scraping and How Can You Use It?*, JetRuby Blog, at https://www.upwork.com/hiring/for-clients/web-scraping-tutorial/

[13] For example, see Robert Bartlet, Adair Morse, Richard Stanton, et al., *Consumer Lending Discrimination in the Era of Fintech*, University of California-Berkley working paper, October 2018, at https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf.

[14] Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications*, November 1, 2017, pp. 33-34, at http://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service.

new data and learning. For example, a principle of securities market regulation in the United States is that, although investors enter capital markets understanding that potential losses are possible, investors should be informed of their risk exposure to make informed investment decisions. Given the complexity and auditing difficulties, sufficiently informing investors and disclosing risks could be challenging when AI- and ML-enabled investment decisions are involved.[15] After a recent case concerning a $20 million automated investment loss, a Stanford University law professor stated, "people tend to assume that algorithms are faster and better decision-makers than human [securities] traders. That may often be true, but when it's not, or when they quickly go astray, investors want someone to blame."[16]

Data Privacy and Identity Fraud Challenges in Artificial Intelligence

Implementing AI-enabled automation in monitoring and reporting activities has potentially problematic implications for privacy and data security. For instance, the role of regulators in ensuring that information gathered on individuals and used by AI to make decisions appropriately respects individuals' privacy is an open question. Additionally, other questions involve how much autonomy AI programs should have when it comes to decisions that might draw the attention of authorities to individuals' financial transactions or lead them to take other adverse actions against individuals, such as closing an account because of a determination that a customer poses too much of a money laundering risk. Further, there is a concern that if erroneous or misinterpreted data is adapted into these systems the faulty information will become ingrained into the algorithms, providing little recourse for the consumer.[17]

As phishing and fraud attacks become more sophisticated, and as large volumes of customer data become more available, AI can be used to effectively identify financial behavior patterns that are irregular for specific customers. For instance, a major American bank receives around 11 million calls a week at its service center and, in order to protect itself from denial of service attacks, the company used a "machine learning-based policy engine [that] blocks more than 120,000 calls per month based on voice firewall policies including harassing callers, robocalls and potential fraudulent calls."[18] While this represents an example of how ML can help defend technology systems from malevolent attacks, there are also concerns that AI can be used to commit identity fraud, including utilizing deepfakes to recreate a person's voice from a short voicemail greeting.[19]

The Future of Work in the Financial Services Industry under Artificial Intelligence

Much like broader concerns about job loss and displacement across the economy, concerns exist about the role of AI in job displacement in the financial services industry, which includes banks, credit unions, insurance, traders, accountants, and consumer-finance entities. According to some estimates, financial services has already ranked in the top three – behind only the information and the manufacturing industries – in terms of the percentage of workers dealing with AI.[20] However, while the financial services workforce is likely to experience rapid change due to AI, some studies have argued that job displacement

[15] Julia Bonafede, Corey Cook, and Glenn Doggett, *Artificial Intelligence and Its Potential Impact on the CFA Institute Code of Ethics and Standards of Professional Conduct*, Chartered Financial Analyst Institute, January 17, 2019, at https://www.cfainstitute.org/en/ethics/codes/std-of-practice-guidance/artificial-intelligence-a-consultation.

[16] Thomas Beardsworth and Nishant Kumar, "Who to Sue When a Robot Loses Your Fortune," Bloomberg, May 5, 2019, at https://www.bloomberglaw.com/document/XA51N7GO000000?bna_news_filter=banking-law&jcsearch=BNA%25200000016a8ce4d6bfadfb9cee2ed10000#jcite (subscription required).

[17] Rich Turrin, *Big Data Gone Bad Shows Why Digital KYC is no Panacea*, Blog, Last accessed June 21, 2019 at https://richturrin.com/big-data-gone-bad-shows-why-digital-kyc-is-no-panacea/

[18] Darrell M. West and John R. Allen, "How artificial intelligence is transforming the world," Brookings Institute, April 24, 2018, at https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/.

[19] LexisNexis Threat Metrix, *Do 'Deepfakes' Mean Real Trouble for Voice Banking?* (February 27, 2019) https://www.threatmetrix.com/digital-identity-blog/mobile/do-deepfakes-mean-real-trouble-voice-banking/.

[20] Craig Desens, "AI Jobs Disruption – Why The U.S. Financial Services Industry Is Different" Dataconomy, Apr. 24, 2019, at https://dataconomy.com/2019/04/ai-jobs-disruption-why-the-u-s-financial-services-industry-is-different/

may include job losses in some categories (e.g. bots replacing customer service representatives) while creating jobs in other categories (e.g. software developers, social media specialists).[21] Some studies have estimated that worldwide by 2030 automation will only displace 15% of workers, and at most 14% of the global workforce will need to switch job categories, even though 60% of jobs will be susceptible to automation.[22] Additionally, researchers are now looking at the increasing prevalence of AI in hiring decisions in larger companies, and how human biases can still be encoded in algorithms.[23]

AI Risk Regulatory Compliance and Risk Management

Risk management and compliance processes at financial institutions currently rely on data to predict whether and how wrong-doing or bad outcomes are occurring or may occur. For example, in anti-money laundering (AML) compliance, financial firms are required to file 'suspicious activity reports' (SARs) with the Treasury's Financial Crimes Enforcement Network (FinCEN) when transactions by a customer appear to potentially be tied to fraud, money laundering, terrorist financing or other transgressions.[24] In connection with the SARs requirement, financial institutions must maintain a compliance program, which may involve training employees to recognize what constitutes suspicious activity and when they are required to file a report. Millions of such reports are filed with FinCEN every year. The agency decides which SARs merit additional attention, an exercise that involves sifting through large data sets to identify patterns that could indicate wrongdoing in financial transactions.

Automation and AI could make performing certain compliance activities, such as AML compliance, more accurate or efficient. A number of commentators have called for greater use of AI (and "regtech," which refers broadly to the adoption of new technologies into regulatory compliance) for a wide range of financial sector risk management and compliance processes that require identifying patterns in data and predicting outcomes. These processes include identity validation for clients, and real-time monitoring, particularly for AML and anti-fraud purposes. They also could include stress testing, risk modeling, economic forecasting and internally monitoring employees (such as, for example, monitoring whether excessively risky trades are harming the bank's own capital or liquidity positions).[25]

Many government and private organizations are already deploying these technologies to some extent. For example, the Financial Industry Regulatory Authority (FINRA)—the front-line self-regulatory organization that monitors securities broker-dealers—has begun to use such tools to surveil the securities market.[26] FINRA predicts that these technologies will help with AML processes, FinCEN's "know your customer" requirements, surveilling employees' trades on behalf of consumers or the firm, managing customer data privacy, preventing security risks, and centralizing supervisory control systems for additional risk management.

[21] Amit Chowdhry, "Artificial Intelligence To Create 58 Million New Jobs By 2022, Says Report," *Forbes*, Sep. 18, 2018, at https://www.forbes.com/sites/amitchowdhry/2018/09/18/artificial-intelligence-to-create-58-million-new-jobs-by-2022-says-report/#510e3c344d4b.

[22] McKinsey Global Institute, "Jobs Lost, Jobs Gained: Workforce Transitions In A Time Of Automation," De. 2017, at https://www.mckinsey.com/~/media/mckinsey/featured%20insights/future%20of%20organizations/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi-jobs-lost-jobs-gained-report-december-6-2017.ashx.

[23] See e.g. "Cornell Professor Ifeoma Ajunwa Discusses Artificial Intelligence Used In Hiring," *National Public Radio*, Apr. 8, 2019, at https://www.npr.org/2019/04/08/711169802/cornell-professor-ifeoma-ajunwa-discusses-artificial-intelligence-used-in-hiring.

[24] See CRS Report R44776, Anti-Money Laundering: An Overview for Congress, by Rena S. Miller and Liana W. Rosen.

[25] For example, see American Bankers Association, "Understanding Regtech," at https://www.aba.com/Tools/Function/Technology/Documents/Understanding-RegTech.pdf.

[26] FINRA, "Technology Based Innovations for Regulatory Compliance ("Regtech") in the Securities Industry, (Sept. 2018), at http://www.finra.org/sites/default/files/2018_RegTech_Report.pdf.