From: Susan Von Struensee
To: 2021-RFI-AI
Subject: [SUSPECTED SPAM] Re: CFPB-2021-0004
Date: Monday, June 21, 2021 10:23:55 PM

CAUTION: This email originated from a non-government domain. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact Cybersecurity Incident Response Team (CSIRT) at 202-435-7200 or report a suspicious email.

Despite the incredible progress and promise made possible by advances in financial artificial intelligence, it nevertheless presents some serious, interconnected risks and limitations.9 Four categories of risks and limitations relating to programming codes, data bias, virtual threats, and systemic risks are particularly noteworthy. Individually and collectively, these four perilous areas loom large as potential inherent and structural dangers in connection with the rise of financial artificial intelligence. A. Uncertain Markets and Artificial Codes Artificial intelligence programs are limited by their underlying code and their ability to fully and properly capture all that is happening in the marketplace. There are simply too many complex, ineffable human and other elements of financial markets and our uncertain world that cannot be fully or properly captured by artificial lines of codes, no matter how comprehensive or smart. As such, computer codes and models frequently make simplifying and oversimplifying assumptions about the workings of the marketplace that can make it appear that it is more predictive and productive than in reality.10 As a result of these simplifications, financial artificial intelligence tools have the capacity to make powerful predictions and to produce incredible value that helps move and grow markets, but on the other hand, they also operate with potentially dangerous blind spots to the workings of the marketplace because of their limitations.11 The fantastical powers and applications of financial artificial intelligence have convinced many within the financial industry to naively believe that these smart machines are the fix for most of our human-created financial problems.12 While such admiration and acclamation is understandable, it must also be balanced with proper recognition of the limitations of artificial intelligence at their underlying codes to perfectly depict and encapsulate the complexities of the financial marketplace and the world at large.13 The 2008 financial crisis was caused and exacerbated in part by too many in the financial industry placing too much faith in smart machines to properly account for the risks and repercussions of a booming—then bursting—real estate market.14 Uncertainty, risk, repercussions, and animal spirits in finance can never be perfectly coded, modeled, mitigated, or eliminated because human unpredictability is beyond precise mathematical modeling and computer coding.15 Furthermore, deal negotiations, board presentations, regulatory actions, legal interpretations, and many other activities critical to finance are done largely among humans communicating using verbal and nonverbal language in ways that smart machines are thus far unable to do on a consistent basis.16 Despite all of its amazing advances, artificial intelligence still does not possess all of the capabilities of the human brain, with its trillions of synaptic connections and billions of neurons.17 Artificial intelligence cannot fully decipher a simple common human phrase like "it's fine," let alone the many nonverbal expressions that humans use among one another.18 In sum, financial artificial intelligence is limited by the incapability of its programming to fully capture the breadth, depth, and diversity of all that is happening in a marketplace. This is due in large part to the whimsical, flawed, and unpredictable role humans continue to play in finance and markets.19 Therefore, as we grow more reliant and assured about the promise of financial artificial intelligence, we should also grow more mindful of its limited capacity to fully comprehend the ineffable complexities of a still largely human-driven marketplace.

B. Discriminatory Data and Algorithmic Biases Discriminatory data and algorithmic bias represent a set of critical risks and limitations associated with financial artificial intelligence. They concern the integrity and utilization of the underlying informational inputs that are the fuel of artificial intelligence systems.20 Most artificial intelligence systems initially need large quantities of data to teach the programs to recognize certain patterns and make certain predictions. At its best, artificial intelligence can uncover valuable new insights and observations from troves of big data, otherwise impossible without artificial intelligence's awesome processing powers.21 At its worst, artificial intelligence can exacerbate misguided old practices and aggravate past social harms with its incredible processing powers and the veneer of novel objectivity since discriminatory humans are associated with the decisions.22 While we should appreciate the incredible potential of financial artificial intelligence, we should also be cognizant of the potential risks inherent in systems built with data that may reflect harmful past biases against the marginalized and the poor that we do not want to replicate in the present or perpetuate in the future.23 We should be particularly mindful of underlying data contexts and applications that are being selected and coded by flawed humans with all of our biases, prejudices, and fallacies.24 First, we should be mindful of the context of the data in order to properly account for potential latent biases. When, where, why, and how was this trove of data generated? Understanding the context of the data is critical to understanding the data, its utility, and its potential risks. Inputting data without properly understanding its context could lead to dangerous discriminatory implications.25 As a crude example, if one obtusely inputs white-collar professional labor data from the 1940s to the 1970s into an artificial intelligence system to predict what demographics of individuals would be the most successful applicants for white-collar professions, the suggestion would likely be white males of a certain age. This is not because the algorithm or code is intentionally pernicious; rather, it is because the underlying data is reflective and reproductive of certain harmful discriminatory practices and (mis)understandings of a bygone era.26 As such, if the context of the data is not properly accounted for, it can lead to innovative technologies that perpetuate old, harmful ways—directly or indirectly via proxy.27 Given the long history of discriminatory practices in the financial industry, adopters of financial artificial intelligence must be particularly mindful of the historical context of the data that they input into their smart systems so as not to bring forth past biases into the present and the future.28 Second, in addition to being more mindful of the context of the data, we should also be more thoughtful about the application of the data by artificial intelligence so as to mitigate potential algorithmic biases.29 Artificial intelligence, as well as its underlying data and code at their most basic level, is amoral, neither immoral nor virtuous. It lacks values and judgments. We imbue these smart machines with the values and judgments that we believe are important, however good or ill the intentions.30 Humans, with all of their foibles and faults, design these systems.31 As such, society cannot simply accept the outputs of artificially intelligent systems without due consideration and understanding of their implications. For example, financial artificial intelligence may recommend that veterans and certain minority populations should be charged higher interest rates on loans without ever considering the social and moral ramifications of such recommendations. Because of the importance of finance in the lives and livelihoods of people, it is critical that programmers, designers, architects, and consumers of financial artificial intelligence systems properly account for the pernicious ways that such systems can be used and misused and must include humans as safeguards in critical decision points.32 In sum, data and algorithmic bias represent one of the key categories of risks and limitations inherent in the rise of financial artificial intelligence. As the financial industry grows more reliant on artificial intelligence, policymakers, regulators, and other key stakeholders must also grow more vigilant about the potential harms that could arise out of data and algorithmic bias. In recent years, there have been significant and serious movements to combat algorithmic bias in finance and beyond.33 Ultimately, it is important that new technology does not bring forth old discriminations into the present and the future under the blended gloss of innovation, neutrality, and objectivity.34

C. Virtual Threats and Cyber Conflicts Another key category of risks and limitations associated with the rise of financial artificial intelligence involves the rise of virtual threats and cyber conflicts in the financial system. The emergence of financial artificial intelligence is an extension of the growing reliance on technology in the financial industry, and this burgeoning reliance has made the financial industry ever more vulnerable to virtual threats. In 2019, IBM found that the finance and insurance industry was the most attacked industry in terms of cybersecurity threats.35 As the financial industry evolves even more into a high-tech industry, it will surely face even more of the same types of cyber challenges confronted by most traditional technology companies.36 The virtual threats against the financial industry can be both external and internal. First, in terms of external virtual threats, financial firms and financial industry regulators must be particularly vigilant against foreign nation-states, competitors, terrorist organizations, cybercriminals, and cybermercenaries.37 In the last decade alone, the financial industry has had to confront a diverse matrix of external threats from state and nonstate actors, some seeking profit while others seeking merely to sow chaos using sophisticated hacks designed to steal billions of dollars, acquire valuable information, and cause significant disruptions.38 Second, in addition to the external threats, financial firms and regulators also have to guard against internal threats, such as rogue employees, corporate spies, and misguided contractors.39 IBM in recent years has estimated that human errors account for a very significant percentage of all data and cybersecurity breaches.40 While such internal threats have always existed within the financial industry, the industry's heavy reliance on technology like artificial intelligence has magnified the impact of such internal threats. In a financial marketplace where millions of dollars can automatically move in fractions of a second with or without a keystroke, the rogue internal threat may be one of the most dangerous menaces to the financial industry.41 Furthermore, both internal and external virtual threats have grown more sophisticated and complex to detect and thwart.42 In the coming years, with the rise of financial artificial intelligence, market regulators and participants may have to confront unprecedented threats in the marketplace. Financial deepfakes, financial fake news, and many other previously unimagined ways to disrupt and manipulate the markets will persist and grow in a marketplace that becomes ever more reliant on technologies like artificial intelligence.43 In 2016, then-Federal Reserve Chair Janet Yellen ominously testified before Congress that cyberattacks on the financial system present "one of the most significant risks our country faces."44 In the last few years alone, hackers injected false data into the U.S. Securities and Exchange Commission's EDGAR electronic filing system and hacked social media accounts to manipulate the stock market.45 For instance, in 2013, cybercriminals hacked the Associated Press's Twitter account to falsely report an attack on the White House, which momentarily caused a $136 billion loss in market value when programs driven by artificial intelligence traded on the bogus news.46 Such innovative, pernicious threats will continue to increase as finance becomes more reliant on automated systems powered by artificial intelligence that may be particularly susceptible to bad or false data as nation-states and nonstate actors try to weaponize technological tools like artificial intelligence that have made so much progress in the financial system possible against the system itself.47 In sum, as the financial industry becomes more like the technology industry, with its greater adoption of artificial intelligence, it will face growing and serious risks concerning virtual and other technology-oriented threats. D. Systemic Risks and Financial Accidents The rise of financial artificial intelligence and related financial technology heightens the dangers of systemic risk and major financial accidents.48 A growing reliance on artificial intelligence and other forms of technology in the financial industry can exacerbate intertwined systemic risks related to size, speed, and interconnectivity. Moreover, the growing complexity of technology increases the risks of serious financial accidents. Wider adoption of financial artificial intelligence can amplify certain systemic risks for the financial system relating to size, speed, and linkage. First, in terms of size, there exists the well-known systemic risk of "too big to fail,"whereby large financial institutions supposedly become too large and important to the welfare of the system to falter or fail.49 As financial artificial intelligence gains more ground in the financial industry, institutions that are critical to the system because of their large data holdings for the purpose of financial artificial intelligence could also become too important to the system to fail. As such, in the future, the systemic risk of size may mean not only the size of a financial institution's balance sheet but also the size of its databases. Second, in terms of speed, wider adoption of financial artificial intelligence would likely lead to even faster financial speeds, which would create a systemic risk of "too fast to save," whereby disruptions, bad acts, and other events could destabilize the financial system before any corrective or preventive measure could be taken.50 During times and trading periods of distress, panic, and confusion, high-speed automated programs running on artificial intelligence can sow greater volatility and calamity by rapidly increasing or decreasing liquidity.51 In the last few decades alone, we have seen unprecedented volatility and flash crashes in the financial markets, made possible by new technology like artificial intelligence.52 Third, in terms of linkage, the prevalence of financial artificial intelligence could intensify the systemic risk of "too linked to fail," whereby actions, errors, and failings trigger destabilizing ripples across the financial system because of the interconnectivity of firms, regardless of their value or size.53 This systemic risk is particularly troubling because of the highly intermediated and interconnected nature of modern finance and the use of similar and interdependent artificial intelligence programs by many firms within the financial industry.54 As a consequence of these tight links and interoperative programs, one or a few firms can create dangerous cycles and cascades of volatility and spillover effects that destabilize the entire financial system.55

In addition to the rise of financial artificial intelligence that exacerbates systemic risk, its ascent could also lead to financial accidents. Charles Perrow, in his landmark study on technological risks Normal Accidents: Living with High-Risk Technologies, theorized that complex technology systems, like the artificial intelligence–driven ones that are at the heart of our financial system, are inherently vulnerable to breakdowns and accidents.56 As financial artificial intelligence grows more prevalent, "normal financial accidents" will likely also grow more frequent within the financial system.57 In fact, both the New York Stock Exchange and the Nasdaq, the two most prominent American stock exchanges, suffered serious malfunctions that halted hundreds of billions of dollars worth of trading for hours during otherwise normal trading sessions in recent years.58 In sum, the proliferation of artificial intelligence in finance increases the dangers of systemic risks and major financial accidents. While we should appreciate the many new positive outgrowths of financial artificial intelligence for certain firms and institutions, we should also be mindful of the hazards and challenges that it may cause for the entire financial system going forward.59

II. KEY IMPLICATIONS AND RECOMMENDATIONS The proliferation of financial artificial intelligence will have many profound implications on finance, law, and society. While the specific and wider effects of financial artificial intelligence remain forthcoming, three particular areas are worthy of closer near-term consideration and action: financial cybersecurity, competition, and societal impact. A. On Financial Cybersecurity One of the most significant issues and challenges arising from the wider adoption of financial artificial intelligence is financial cybersecurity. Today, many of the more sophisticated attempts to manipulate and disrupt financial markets take place exclusively in cyberspace and are aimed at artificial intelligence systems.60 Because financial artificial intelligence relies on interconnected, complex technological systems, being able to safeguard those systems from threats and attacks is critical to preserving the integrity of the financial system.61 One of the critical challenges concerning financial cybersecurity is that disparate private parties, who may have misaligned and competing interests, control much of the global cyberinfrastructure.62 As such, private firms motivated by higher profits, competitive advantage, expense reductions, and other understandable considerations may not always act with systemic financial cybersecurity as a top

priority in their decision-making.63 For instance, many financial firms already spend substantial sums of money annually on regulatory compliance and cybersecurity efforts and may be reluctant to spend more on a timely basis going forward.64 That said, sound systemic financial cybersecurity requires all or most firms to have strong cybersecurity capabilities. It is not nearly enough for just a few firms to have strong cybersecurity safeguards while their counterparties and vendors are vulnerable, given the interconnected nature of the modern financial system. As such, public policymakers need to think creatively to incentivize private firms around the world to innovate faster and cooperate better with other firms and public regulators as the specter of cybersecurity attacks grows larger with advances in financial artificial intelligence.65

Ultimately, sound and sustainable financial cybersecurity requires smart leadership and partnership from both the public and private sectors.66 As then-President Barack Obama remarked in 2015 about cybersecurity, "neither government, nor the private sector can defend the nation alone. It's going to have to be a shared mission—government and industry working hand in hand, as partners."67 In the absence of such coordinated action, the integrity of the financial system could come into question as institutions and investors lose trust and faith in the stability and reliability of the financial system.68 This is particularly true with the rise of financial artificial intelligence because of its heavy reliance on electronic networks and computerized systems for its operations. Furthermore, many financial artificial intelligence systems are "black box" systems, meaning that their operations are difficult or impossible to fully understand, explain, or audit.69 In sum, wider adoption of financial artificial intelligence will have serious ramifications on the cybersecurity and integrity of the global financial marketplace. Private and public institutions throughout the world must act with greater speed and coordination to guard against the looming threats of cyberattacks, manipulation, and other bad acts that strike at the heart of the modern, high-tech financial system.70 It should be noted that while such urgency may be clear and present, it does not necessarily mean that such urgency would manifest in swift and smart policies and actions given various geopolitical complexities involved in a vexing issue like financial cybersecurity.71

B. On Competition The rise of financial artificial intelligence will have significant implications for competition within the financial industry and the greater economy. Because artificial intelligence is highly dependent on large data sets for insights, firms with captive, large sets of data built into their structural platforms may end up having a durable competitive advantage in the marketplace that ultimately hurts consumer welfare and the competitive landscape of finance.72 The ongoing debates and investigations concerning competition and antitrust among large technology companies like Google, Amazon, and Facebook may soon spill over into the financial industry with large financial institutions, which are functionally large technology companies similarly powered by large troves of data.73 In recent years, large financial institutions like JPMorgan Chase have reportedly hired more software developers and technologists than Google or Microsoft.74 Technological innovations and advances have been dramatically changing the financial industry.75 The ascent of financial artificial intelligence is an important extension of this ongoing sea change. New financial technology and artificial intelligence have transformed many segments of modern finance. In trading, smart machines powered by artificial intelligence now trade most securities in global finance, often doing so better, cheaper, and faster than their human counterparts.76 In risk management, many, if not most, large financial institutions use financial artificial intelligence programs to aid them in managing risk.77 BlackRock, the world's largest asset management company, with trillions of dollars under management, uses Aladdin, a proprietary artificial intelligence program to manage risk for its clients. Most significant financial institutions use artificial intelligence programs in their financial research efforts as well.78 For instance, such programs can be coded to analyze market trends, read breaking news, and spot investment opportunities entirely on their own.79 Finally, in wealth management, artificial intelligence programs can manage funds just as well as many financial advisors—at a fraction of the cost. New financial technology companies, like Wealthfront and Betterment, use artificial intelligence programs to advise and manage billions of dollars of assets for clients at lower costs with comparable returns, all from an app on one's phone.80 While all of the aforementioned innovations and advances made possible by artificial intelligence have created many benefits, they also raise legitimate concerns about competition in ways historically unconsidered or underappreciated by banking and antitrust regulators.81 Because the technology and data underlying much of financial artificial intelligence requires significant investments and favors the data-rich, there is appropriate concern that early movers and better-resourced institutions would acquire durable competitive advantages that ultimately stifle innovation, eliminate meaningful competition, and harm consumer welfare.82 It is not difficult to foresee a financial firm acquiring and leveraging its superior data in terms of quality and quantity, as well as concentrated network effects, to build an economic moat to shield itself from competition in the same manner as its more traditional technology-oriented counterparts.83 Similar to current concerns relating to the domination of Google, Amazon, and Facebook in their respective technological territories in search, online commerce, and social media, there is good reason to believe that some large, dominant financial institutions may warrant similar scrutiny with the rise of financial artificial intelligence in the coming years.84 Whereas federal and state regulars are currently focused on large, traditional technology companies for their anticompetitive practices and implications, in the near future such regulators may turn a similar investigatory gaze on financial institutions given the rise of financial artificial intelligence and its implications for competition within the financial industry.85

Therefore, as artificial intelligence becomes more common in finance, policymakers must grow more watchful, thoughtful, and action-oriented about the potential implications it may have for competition within the industry and beyond.86 C. On Societal Impact The rise of financial artificial intelligence will likely have a profound societal and economic impact on an individual as well as a collective basis.87 On an individual basis, the rise of artificial intelligence in finance raises important questions about the role of humans in finance. On a collective basis, the ascent of financial artificial intelligence also raises important questions about the role and purpose of finance in society. First, on an individual basis, financial artificial intelligence has profound implications for people working in finance, just as similar ramifications are unfolding in other sectors of our economy.88 Artificial intelligence has gradually—then rapidly—displaced much human labor and effort in finance, and understandably so.89 Smart machines driven by artificial intelligence with perfect memory and recall can process large volumes of data faster, cheaper, and more accurately than humans in most circumstances, and they do not tire with more work or grow irrational with "animal spirits" the way humans normally do.90 It is worth noting that while artificial intelligence has reduced and eliminated many jobs in finance and beyond, it has also produced new jobs, some of which are highly desirable and others that are less so.91 Despite the undeniable and impressive rise of financial artificial intelligence, humans will likely remain the critical players in modern finance (for now) because of their judgment and sophistication, especially as it relates to other humans.92 More importantly, human engagement that touches on emotions, ethics, values, empathy, culture, and other basic human traits remains critical to the success and failure of any financial endeavor. Smart machines, although artificially intelligent, still need humans to build their initial codes and hardware as well as embed them with human values and ethics.93 Moreover, humans can nevertheless override their smart machines in many situations. As such, in many circumstances, artificial intelligence is often outmatched by natural stupidity or natural brilliance. Ultimately, on an individual basis, financial artificial intelligence will become an even more critical technological ally for humans in finance and not their adversary. This will be the case for both government financial regulators and those they regulate.94 The important questions in the face of these rapid technological changes in finance and beyond are less about what artificial intelligence is going to do to humans; rather, they are more about what humans are going to do with artificial intelligence going forward to make one another even better and more powerful.95 Second, on a collective basis, financial artificial intelligence implicates significant questions about the proper role of finance in society. As finance continues to adopt new technologies like artificial intelligence, it can sometimes lose sight of the fact that finance at its core—behind and beyond all the high-tech gadgetries, complex codes, and seas of data—is driven by real people and real social purposes.96 Faster, cheaper, bigger, and more efficient finance does not necessarily mean a more just and socially valuable form of finance.97 Frequently in discussing matters of finance, scholars, regulators, and policymakers forget that people and communities are at the heart of finance and markets.98 People create supply and demand. People move markets. It is flesh and blood people who need finance and financing for education, homes, health care, investments, and other life and social pursuits.99 Finance is ultimately a tool of social utility and connection that would lose much of its meaning without the context of people and society.100 One of the critical responsibilities for executives, policymakers, and regulators in the years ahead centers on how better to update a twentiethcentury financial system to account for twenty-first-century financial advances like artificial intelligence without losing focus on the humanoriented missions of finance and democratic values like equal access and transparency.101 Doing so will not be easy given the serious challenges of modern politics, old narratives, and scarce resources.102 Furthermore, the objectives of regulating new financial technology can often be crosscutting, whereby achieving one objective like greater transparency could undercut other objectives like efficiency and fairness.103 That said, properly recognizing the human heart of finance is key to better understanding and harnessing the power of financial artificial intelligence for positive monetary and social impact, while taming its hostilities.104 To legislate, regulate, innovate, and act on finance divorced from its human participants, beneficiaries, and victims—while theoretically elegant—can lead to serious negative consequences.105 In fact, as noted earlier, in the run up to the financial crisis of 2008, too many regulators and firms placed too much faith in the elegant models of smart machines and lost focus on the real-world implications of finance and markets to the detriment of society.106 In sum, as finance grows more reliant on new technologies like artificial intelligence, key financial stakeholders must grow more vigilant in safeguarding the people-centered, social purposes of finance.107

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3480607

On Sat, Jun 19, 2021 at 2:58 PM Susan Von Struensee <susanvonstruensee@gmail.com> wrote:

> COMMENTS OF SUSAN VON STRUENSEE, JD, MPH
>
> to the
>
> Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning
>
> 86 FR 16837-38 (March 31, 2021)
>
> Agency/Docket Numbers:
>
> Docket ID OCC-2020-0049
>
> Docket No. OP-1743
>
> Docket No. CFPB-2021-0004
>
> Docket No. NCUA-2021-0023
>
> # Oversight of Third Parties
>
> > Financial institutions may opt to use AI developed by third parties, rather than develop the approach internally. Existing agency guidance (as noted in the Appendix) describes information and risks that may be relevant to financial institutions when selecting third-party approaches (including ones using AI) and sets out principles for the validation of such third-party approaches.
>
> *Question 10:* Please describe any particular challenges or impediments financial institutions face in using AI developed or provided by third parties and a description of how financial institutions manage the associated risks. Please provide detail on any challenges or impediments. How do those challenges or impediments vary by financial institution size and complexity?
>
> The consideration of third parties in AI is wide and various.
>
> 1. AI EQUITY

As AI becomes increasingly pervasive, there has been growing and warranted concern over the effects of this technology on society. To fully understand these effects, however, one must closely examine the AI development process itself, which impacts society both directly and through the models it creates. The attached white paper, "Responsible Sourcing of Data Enrichment Services," addresses an often overlooked aspect of the development process and what AI practitioners can do to help improve it: the working conditions of data enrichment professionals, without whom the value being generated by AI would be impossible. This paper's recommendations will be an integral part of the shared prosperity targets being developed by Partnership on AI (PAI) as outlined in the AI and Shared Prosperity Initiative's Agenda.

High-precision AI models are dependent on clean and labeled datasets. While obtaining and enriching data so it can be used to train models is sometimes perceived as a simple means to an end, this process is highly labor-intensive and often requires data enrichment workers to review, classify, and otherwise manage massive amounts of data. Despite the foundational role played by these data enrichment professionals, a growing body of research reveals the precarious working conditions these workers face. This may be the result of efforts to hide AI's dependence on this large labor force when celebrating the efficiency gains of technology. Out of sight is also out of mind, which can have deleterious consequences for those being ignored.

As just one example, as evident from the attached report The development and deployment of Artificial Intelligence (AI) systems relies on the cognition of human workers whose judgment and intelligence are widely employed to build the datasets used to train and validate models and ensure reliable real-time performance. This work ranges from preparing, cleaning, and labeling training data to providing human review of algorithmic outputs such as low-confidence predictions. For the purpose of this white paper, we refer to all of these tasks as "data enrichment work." The increase in AI development has given rise to a parallel industry in data enrichment work which serves as a growing source of jobs, particularly in the Global South. Existing research on data enrichment professionals reveals the precarious working conditions they operate under. Workers often face inconsistent and inappropriate pricings for their work, unclear instructions, lack of recognition, and emotional and physical stress related to long and ad-hoc working hours and exposure to graphic content. Some of these challenges are inherent to the work itself while others are shaped by company architectures, software used to mediate the work, business models, and client and vendor behavior. As the AI industry and the data enrichment workforce it relies on continue to grow, it is increasingly important to critically evaluate the conditions under which this work is being done. In particular, ensuring that these jobs are of a decent quality and provide for a decent level of worker well-being is crucial. Though there are many stakeholders in the industry that can and should play a role in ensuring favorable working conditions in the data enrichment industry—including policymakers, labor unions, civil society, investors, and company executives—this white paper focuses on the role of the immediate clients of data enrichment services. Clients making the day-to-day decisions related to sourcing data enrichment work for AI projects (such as product and program managers, AI developers, and data scientists) often shape the working conditions of data enrichment professionals and thus are in a position to directly make improvements. Today, the data enrichment ecosystem is complex and unstandardized with few resources that clients can turn to for guidance on how to take concern for worker well-being into account when making sourcing decisions and how to incorporate practices that benefit workers. This has created a situation where, even if a client wants to make decisions that are mindful of their impact on workers' experiences, it is not easy for them to do so. This white paper aims to make it simpler for clients to navigate this complex ecosystem, critically evaluate how their decisions may be impacting worker experience, and position themselves to develop better practices that benefit workers. The paper offers considerations for clients as they navigate the full process of sourcing and managing data enrichment work, from selecting a data enrichment service provider to writing instructions, setting up payment terms, and finally offboarding workers.

2. AI STIMULATE INNOVATION

Finance has been transformed by digitalization and datafication over the past five decades. The latest wave of technology in finance (Fintech) is re-shaping the sector at an unprecedented pace. This digital financial transformation brings about structural changes, with positive and negative effects, likely even more in the high-potential markets of the Middle East and North Africa.

Fintech can stimulate competition and product variety with positive outcomes for societies and economies. The fundamental changes taking place in the financial system, however, call for the design of adequate approaches to Fintech innovation. An ecosystem is required that allows innovation balanced with financial inclusion, financial stability, market integrity and consumer protection.

This toolkit presents novel regulatory and market approaches policymakers, regulators, and development professionals can adopt to enable safe Fintech innovation.

Regulatory frameworks will determine the future of Fintech. Following principles from global good practice (mainly activity-based, proportional, and technology-neutral regulation), regulatory approaches in sequenced stages help to create pathways for innovative Fintech firms.

First, regulators ought to identify and modernize unsuitable regulation based on a regulatory impact assessment that determines whether legacy rules remain useful.

Second, proportional regulation, reflected in provisions for market stability and integrity depending on the extent of risks underlying the regulated activity, create supportive pathways for new, particularly inclusive non-bank financial services.

Third, an Innovation Hub with experts of the regulatory authority is best suited to guide Fintech firms through the regulatory maze, yield valuable insights into market innovations, and assess possibilities of dispensation.

Fourth, testing and piloting regimes allow to apply leniency in a wait-and-see or test-and-learn approach to assist innovative firms. Authorities can further decide to tolerate innovations by licensed institutions and possibly by start-ups by extending on a case-by-case basis waivers or no-action-letters which declare certain activities as permissible or suspend certain rules.

Fifth, a regulatory sandbox, which standardizes the scope of testing and piloting, allows regulators to create a tightly defined safe space for granting dispensation from specific regulatory requirements for innovative firms that qualify.

Sixth, restricted licences allow feasible innovative firms to further develop their client base and financial and operational resources in a controlled manner.

Seventh, a full licence is essential for innovative firms as size requires and permits. Over these stages, as regulatory rigour and costs increase so tend to do Fintech firms' maturity and ability to cope with risks and compliance, while maintaining a level playing field for licensed entities.

Demand and supply side factors will eventually propel innovative entrepreneurship and Fintech growth. Market approaches to Fintech innovation combine the support of financial and digital literacy in the population, cybersecurity capacities in the sector, acceleration programmes and investor-friendliness in the business environment, and technology clusters or digital centres in public-private- academic partnerships.

Sequenced reforms that are informed by global good practise, responsive to the local context and that contribute to regionally consistent frameworks, are policymakers best pick in support of an enabling ecosystem for Fintech. Concerted efforts will enable innovative financial service providers to tap the market and scale as well as Fintech to be beneficial for financial inclusion, competition and economic development across the region.

Zetzsche, Dirk Andreas and Arner, Douglas W. and Buckley, Ross P. and Kaiser-Yücel, Attila, Fintech Toolkit: Smart Regulatory and Market Approaches to Financial Technology Innovation (May 11, 2020). University of Hong Kong Faculty of Law Research Paper No. 2020/027, Available at SSRN: https://ssrn.com/abstract=3598142 or http://dx.doi.org/10.2139/ssrn.3598142

Even in an increasingly digital world, people have a right to engage in private financial transactions. Cryptocurrency offers a way to bring to the online world some of the civil liberties benefits that people have long enjoyed when using cash.

The ability to transact anonymously is instrumental to protecting Americans' civil liberties. Anonymity is important precisely because financial records can be deeply personal and revealing: they provide an intimate window into a person's life, revealing familial, political, professional, religious, and sexual associations—what organizations a person donates to, what family members a person supports, what services a person pays for, and what books and products a person buys. The ability to transact anonymously allows people to engage in First Amendment–protected political activities, including attending public protests and donating to advocacy organizations—activities that may be sensitive or controversial. As just one example, photos from the recent Hong Kong prodemocracy protests showed long lines at subway stations as protestors waited to purchase tickets with cash so that their electronic purchases would not place them at the scene of the protest. These photos underscore the importance of anonymous transactions for civil liberties. For the same reasons, dissidents in Belarus protesting to the reelection of the president and protestors in Nigeria campaigning against police brutality turned to cryptocurrency. Those anonymous transactions should be protected whether those transactions occur in the physical world with cash or online.

Cryptocurrency is also important for civil liberties because it is resistant to censorship. For years, NGOs such as the Electronic Fronteir Foundation has documented examples of traditional financial intermediaries shutting down accounts in order to censor otherwise legal speech. For example, financial intermediaries have cut off access to financial services for social networks, independent booksellers, and whistleblower websites, even when these websites are engaged in First Amendment–protected speech. In some of those cases of financial censorship, the censored organization has turned to cryptocurrency in order to continue to do business. For that reason, cryptocurrency transactions are generally more sensitive than other financial transactions. Cryptocurrencies have served as a vital lifeline for websites and online speakers who find themselves suddenly in the bad graces of a traditional payment intermediary, and who often have no other recourse. For those who seek to support these online speakers, cryptocurrencies may offer a privacy-protective, reliable alternative to financial channels governed by extra-legal policies of corporations. See Electronic Frontier Foundation, Financial Censorship, available at https://www.eff.org/issues/financialcensorship.; Jeremy Malcolm, Payment Processors Are Still Policing Your Sex Life, and the Latest Victim Is FetLife, Electronic Frontier Foundation (Mar. 15, 2017), available at https://www.eff.org/deeplinks/2017/03/payment-processors-are-still-policing-your-sex-life. ; Rainey Reitman, Legal Censorship: PayPal Makes a Habit of Deciding What Users Can Read, Electronic Frontier Foundation (Aug. 21, 2018), available at https://www.eff.org/deeplinks/2012/02/legal-censorshippaypal-makes-habit-deciding-what-users-can-read.

Please meet directly with innovators, technology users, and civil liberties advocates prior to implementing any regulations. Many people make donations through Bitcoin, Ethereum, Zcash, Litecoin, Dash, Dai, and other cryptocurrencies, including directly to non profits' wallets.Like the open Internet, cryptocurrency networks are a form of open source innovation that can enhance the freedom and privacy of technology users.

A database can become a honeypot of information that tempts bad actors, or those who might misuse it beyond its original intended use. Thousands of FinCEN's files were recently exposed to the

public, making it clear that FinCEN's security protocols are not adequate to prevent even large-scale leakage.This is not the first time that a sensitive government database has been leaked, mishandled, or otherwise breached. Over the past several weeks, the SolarWinds hack of U.S. government agencies has made headlines, and details are still emerging.As just a few other examples, a hack of the Office of Personnel Management exposed over 22 million personnel records and a breach of a voting records database led to the personal information of over 190 million Americans being published online. It's clear that government databases can and frequently do suffer from data breaches—whether through intentional leaks, hacks by bad actors, or negligent security practices—and thus the government should avoid collecting and storing unnecessary data. This is especially true for data as sensitive as the physical locations and identities of individuals associated with their financial transactions.

While 1970s-era court opinions held that consumers lose their privacy rights in the data they entrust with third parties, modern courts have become skeptical of these pre-digital decisions and have begun to draw different boundaries around our expectations of privacy. Acknowledging that our world is increasingly digital and that surveillance has become cheaper and more ubiquitous, the Supreme Court has begun to chip away at the third-party doctrine—the idea that an individual does not have a right to privacy in data shared with a third party. Some Supreme Court Justices have written that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." In 1976, the Supreme Court pointed to the third-party doctrine in holding in U.S. v. Miller that the then-existing Bank Secrecy Act reporting requirements did not violate the Fourth Amendment.

Two developments make continued reliance on the third-party doctrine suspect, including as the source for regulations such as those contemplated here. First, since the Miller decision, the government has greatly expanded the Bank Secrecy Act's reach and its intrusiveness on individual financial privacy. Although the Supreme Court upheld the 1970s regulations in an as-applied challenge, Justice Powell, who authored Miller, was skeptical that more intrusive rules would pass constitutional muster. In California Bankers Association v. Shultz, Justice Powell wrote, "Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy." Government intrusion into financial privacy has dramatically increased since Miller and Shultz, likely intruding on society's legitimate expectations of privacy and more directly conflicting with the Fourth Amendment. Second, since Miller, we have seen strong pro-privacy opinions issued from the U.S. Supreme Court in multiple cases involving digital technology that reject the government's misplaced reliance on the third-party doctrine. This includes: U.S. v. Jones (2012), in which the Court found that law enforcement use of a GPS location device to continuously track a vehicle over time was a search under the Fourth Amendment; Riley v. California (2014), in which the Court held that warrantless search and seizure of the data on a cell phone upon arrest was unconstitutional; and Carpenter v. U.S., in which the Court held that police must obtain a warrant before accessing cell site location information from a cell phone company. These are steps by the courts to better recognize that Americans do not sacrifice their privacy rights when interacting in our modern society, which is increasingly intermediated by corporations holding sensitive data. This understanding of privacy can and should extend to our financial data.
https://www.eff.org/files/2021/01/04/electronic_frontier_foundation_comments_to_fincen_on_requirements_for_certain_transactions_involving_convertible_virtual_currency_and_digital_assets.pdf

The expanded reach of AI in FinTech will interact in novel ways with existing privacy and data protection law outside the United States. Obtaining the identity of the owner of a wallet can reveal the wallet owner's previous transaction records, allowing precise conclusions concerning the private lives and financial habits of the individuals concerned. While such disclosures' asserted purpose is to "verify the identity of the customer," it clearly involves or requires the disclosure or processing of a wider set of data: it cannot be treated as merely obtaining the wallet owner's identity. As such, government access to such data may trigger legal safeguards under international and foreign laws, including independent judicial authorization, legal and factual elements demonstrating that the disclosure of information is relevant to the criminal investigation and particular transactions, the respect of the principles of necessity and proportionality, public transparency reporting and oversight mechanisms, mandatory notification to the targeted individual at the earliest opportunity to ensure access to remedies, and a fixed list of information that a request must contain so providers can challenge and reject disproportionate or unnecessary demands. For guidance, critical safeguards rooted in international human rights law are identified in the Necessary and Proportionate Principles on the Application of Human Rights, its global and Inter-American Legal analysis, and Privacy International Guide to International law, as well as in the recent case law of the European Court of Human Rights concerning the Protection of Personal Data. Necessary and Proportionate Coalition, Global Legal Analysis (May 2014), available at http://necessaryandproportionate.org/global-legal-analysis; Privacy International, Guide to International Law and Surveillance 2.0 (Feb. 2019), available at https://privacyinternational.org/sites/default/files/2019- 04/Guide%20to%20International%20Law%20and%20Surveillance%202.0.pdf; Katitza Rodriguez et al., The Inter-American Legal Analysis, Derechos Digitales and Electronic Frontier Foundation, available at https://necessaryandproportionate.org/americas-legal-analysis.

How will regulations seek to resolve such potential conflicts of law between the United States and other jurisdictions? Please consult with colleagues at the European Data Protection Board and comparable institutions internationally, and make clear how the proposals will respect the necessity and proportionality requirements of international law, and the data protection regulations of other countries. Without such clarity, there is a risk that the enforcement of these broader regulations would lead to legal challenges in Europe and elsewhere and create legal uncertainty for the affected institutions.

And further regarding third parties, please ensure there are not steps taken that create unintended consequences for Blockchain Technology, chilling innovation, for smart contracts and other decentralized technology with a wide range of lawful uses.

Wallets that banks transact with are not always tied to particular humans; in reality, many such wallets will be part of an automated system with which the user transacts. Despite the name, "wallets" are not just personal stores of currency tied to particular individuals: they are often a way for computing systems to hold and dispense money without relying on institutions. Blockchain technologies such as "smart contracts" enable the automatic execution of transactions between wallets without necessarily requiring the involvement of intermediaries or the involvement of humans at all. Wallets are not always caches of digital money held by users; rather, a wallet is often one link in a chain through which an automated, frictionless transaction is executed. Tokens stored in "wallets" may represent more than just money—they may, for example, be tied to permissions and unlocking requirements around personal data, or they may provide transparency into the automatic execution of an agreement when a condition is met. "Smart contracts" can be conceptually simplified to "programmable money," and have a wide range of lawful use cases beyond basic financial transactions. Being able to send value directly to others with no intermediary enables programmers to write computer code that automatically transfers value when a condition is met. As one example, in the music industry, decentralized applications like Audius already use smart contracts to transfer money from users directly to musicians—automatically, and without any intermediary between the user and the musicians.

We are in the very earliest days of the exploration of smart contract technology. Just as it would have been an error to see the early Internet as merely an extension of the existing postal service, it is important not to view the risks and opportunities of smart contracts strictly through the lens of financial services. Any regulation in this space needs input from the industry and experts—to avoid unintended consequences for a broad swath of emerging technologies.

We also need to consider decentralized exchanges, a new technology utilizing smart contracts that seeks to address consumer needs that are not being met by existing financial services. Many people obtain digital currencies through centralized cryptocurrency exchanges. Blockchains themselves are decentralized, and transactions on blockchains are resistant to censorship. However, centralized exchanges act as choke-points through which users must pass to begin participating in the network; thus, financial censorship is most easily conducted at centralized exchanges. We have already seen examples of centralized exchanges mishandling user funds and betraying the trust of customers. Centralized exchanges can freeze the funds of customers, block certain customers from the platform, or block specific transactions, with no obligations to provide affected customers with an appeals process. Centralized exchanges can suffer outages, hacks, or losses that prevent customers from accessing their digital currencies. These centralized exchanges are also a target for criminals seeking to steal customer funds, and can themselves be run by unscrupulous individuals who abuse their access to customer funds and data.

Decentralized exchanges, by contrast, allow for the peer-to-peer exchange of digital currencies using smart contracts. For example, requests to sell and purchase cryptocurrency can be submitted to a smart contract that matches and completes these exchange transactions. Decentralized exchanges generally do not need to hold funds for customers; rather, customers maintain possession of their cryptocurrency, and the decentralized exchange can automatically execute exchange transactions without taking possession of the assets. Decentralized exchanges thus generally do not possess a central honeypot of money that might attract criminals like centralized exchanges do, and cannot themselves steal funds. Because transactions on decentralized exchanges do not require an intermediary, they cannot be easily censored by a single entity. Decentralized exchanges are an area of rapid research and innovation, and many cryptographers and programmers are experimenting with other trustless smart contract applications that may have significant public benefit in the long term.

We wish to avoid steps interfering with the growing ecosystem of smart contract technology, including decentralized exchanges. Let's not chill experimentation in a field that could have many potential benefits for consumers, and let's not prevent American users and companies from participating when those systems are deployed in other jurisdictions.

3. AI Algorithms between users, developers, regulators and consumers

As the attached paper shows, AI in finance comes with three regulatory challenges: (1) AI increases information asymmetries regarding the capabilities and effects of algorithms between users, developers, regulators and consumers; (2) AI enhances data dependencies as different day's data sources may may alter operations, effects and impact; and (3) AI enhances interdependency, in that systems can interact with unexpected consequences, enhancing or diminishing effectiveness, impact and explainability. These issues are often summarized as the "black box" problem: no one understands how some AI operates or why it has done what it has done, rendering accountability impossible.

Even if regulatory authorities possessed unlimited resources and expertise – which they clearly do not – regulating the impact of AI by traditional means is challenging.

To address this challenge, strengthen the internal governance of regulated financial market participants through external regulation. Part IV thus suggests that the most effective path forward involves regulatory approaches which bring the human into the loop, enhancing internal governance through external regulation.

In the context of finance, the post-Crisis focus on personal and managerial responsibility systems provide a unique and important external framework to enhance internal responsibility in the context of AI, by putting a human in the loop through regulatory responsibility, augmented in some cases with AI review panels. This approach – AI-tailored manager responsibility frameworks, augmented in some cases by independent AI review committees, as enhancements to the traditional three lines of defence – is likely to be the most effective means for addressing AI-related issues not only in finance – particularly "black box" problems – but potentially in any regulated industry.

Zetzsche, Dirk Andreas and Arner, Douglas W. and Buckley, Ross P. and Tang, Brian, Artificial Intelligence in Finance: Putting the Human in the Loop (February 1, 2020). CFTE Academic Paper Series: Centre for Finance, Technology and Entrepreneurship, no. 1., University of Hong Kong Faculty of Law Research Paper No. 2020/006, Available at SSRN: https://ssrn.com/abstract=3531711

Keywords: fintech, regtech, artificial intelligence, human in the loop, financial regulation

I appreciate the opportunity to submit comments.

Respectfully Submitted,

Susan von Struensee, JD, MPH