From: Susan Von Struensee [redacted]
Sent: Saturday, June 19, 2021 2:58 PM
To: Comments
Subject: [EXTERNAL MESSAGE] Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning RIN 3064–ZA24
Attachments: electronic_frontier_foundation_comments_to_fincen_on_requirements_for_certain_transactions_involving_convertible_virtual_currency_and_digital_assets.pdf; PAI-Responsible-Sourcing-of-Data-Enrichment-Services.pdf; SSRN-id3531711.pdf; SSRN-id3598142.pdf; svsinnovatefintech.pdf

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

January 4, 2021

VIA ELECTRONIC FILING

Policy Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

FinCEN Docket No. FINCEN-2020-0020, RIN 1506-AB47

Comments to the Financial Crimes Enforcement Network (FinCEN) on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

I. Introduction

The Electronic Frontier Foundation (EFF) respectfully submits this letter to voice its concerns about FinCEN's proposal to implement certain recordkeeping and reporting requirements for cryptocurrency transactions.[1] The proposed rule would require money service businesses such as cryptocurrency exchanges to collect identity data not just about their own customers, but also about non-customers who transact with their customers using their own cryptocurrency wallets. The rule would require regulated businesses to keep records of cryptocurrency transactions over $3,000 USD and to report cryptocurrency transactions over $10,000 USD to the government.

EFF is concerned that the proposed regulation would (1) undermine the civil liberties of cryptocurrency users, (2) give the government access to troves of sensitive financial data beyond what is contemplated by the regulation, (4) violate the Fourth Amendment, (5) fail to comply with international privacy standards, and (6) present unintended consequences for certain blockchain technology—such as smart contracts and decentralized exchanges—that could chill innovation. Based on the substantial potential harms of this proposed regulation, EFF urges FinCEN not to implement this proposal.

EFF is also troubled that the proposal appears to be a transparent attempt to push a midnight regulation through before the end of the current presidential administration. The unusually short comment period over the winter holiday means that many experts

[1] Financial Crimes Enforcement Network, U.S. Treasury Department, *Notice of Proposed Rulemaking*, *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*, available at https://www.federalregister.gov/public-inspection/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets.

and other members of the public will not have the opportunity to provide feedback on the potentially enormous consequences of this regulation. We urge FinCEN to significantly extend the comment period to a minimum of 60 days as well as to offer additional time for comments after it makes any adjustments to the proposed regulation. We also urge FinCEN to meet directly with innovators, technology users, and civil liberties advocates prior to implementing any regulations.

II. About the Electronic Frontier Foundation

EFF is a nonprofit civil liberties law and technology organization. Founded in 1990, EFF champions individual privacy, free expression, and innovation. With more than 35,000 members worldwide, EFF uses public education campaigns, impact litigation, open source technology projects, policy analysis, and grassroots activism to ensure that civil liberties are protected in the digital age.

EFF has been at the forefront of identifying and advocating for civil liberties issues implicated by emerging technologies since its founding. For example, in the 1990s, EFF successfully challenged—in the courts and in policy discussions—broad export controls that attempted to limit the distribution of strong public key encryption, a technology that now underlies the security of the modern Internet and the financial transactions that take place across it. In *Bernstein v. United States*—in which EFF served as counsel to the plaintiff—the Ninth Circuit Court of Appeals ruled that computer code is speech protected by the First Amendment and that laws restricting its publication are unconstitutional. This foundational legal concept helped shape the thriving technological ecosystem in the United States today. EFF has also brought litigation challenging unconstitutional surveillance, including lawsuits challenging National Security Letters and certain warrantless mass surveillance programs of the National Security Agency. In addition, EFF's groundbreaking technology projects help to enhance security and protect privacy; for example, EFF's Certbot is a tool used by more than 20 million websites to encrypt content and protect their users' privacy and security, and EFF's Privacy Badger defends web browser users from being secretly tracked by advertisers and other third parties.

EFF allows its supporters to make donations through Bitcoin, Ethereum, Zcash, Litecoin, Dash, Dai, and other cryptocurrencies, including directly to EFF's wallets. EFF has provided testimony and public comments[2] on proposed cryptocurrency regulations in

[2] Electronic Frontier Foundation, *EFF, Internet Archive, and Reddit Oppose New York's BitLicense Proposal* (Oct. 21, 2014), available at https://www.eff.org/press/releases/eff-internet-archive-and-reddit-oppose-new-yorks-bitlicense-proposal; Rainey Reitman, *EFF and Open Rights Group Defend the Right to Publish Open Source Code to the UK Government*, Electronic Frontier Foundation (Aug. 16, 2019), available at https://www.eff.org/deeplinks/2019/06/eff-and-open-rights-group-defend-right-publish-open-source-software-uk-government; Rainey Reitman, *SEC's Action Against Decentralized Exchange Raises Constitutional Questions*, Electronic Frontier Foundation (Feb. 12, 2019), available at https://www.eff.org/deeplinks/2019/02/secs-action-against-decentralized-exchange-raises-constitutional-questions.

the past to voice the concerns of technology users, innovators, and civil liberties advocates.

Like the open Internet, cryptocurrency networks are a form of open source innovation that can enhance the freedom and privacy of technology users. EFF's mission to ensure that technology supports freedom, justice, and innovation is directly implicated by proposed regulations that would derail new cryptocurrency innovation, increase government surveillance, and hamper the civil liberties of technology users.

III. The Proposed Regulation Would Undermine the Civil Liberties of Cryptocurrency Users

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 proposed regulation would undermine these civil liberties benefits.

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 pro-democracy 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[3] and protestors in Nigeria campaigning against police brutality[4] 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, EFF has documented[5] 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

[3] Anna Baydakova, *Belarus Nonprofit Helps Protestors With Bitcoin Grants*, CoinDesk (Sep. 9, 2020), available at https://www.coindesk.com/belarus-dissidents-bitcoin.
[4] Sandali Handagama, *Nigeria Protests Show Bitcoin Adoption Is Not Coming: It's Here*, CoinDesk (Oct. 21, 2020), available at https://www.coindesk.com/nigeria-bitcoin-adoption.
[5] Electronic Frontier Foundation, *Financial Censorship*, available at https://www.eff.org/issues/financial-censorship.

networks,[6] independent booksellers,[7] and whistleblower websites,[8] 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.

The proposed regulation would require money service businesses such as cryptocurrency exchanges to collect identity data about non-customers who transact with their customers using their own cryptocurrency wallets. The proposed regulation would require these services to keep that data and to provide it to the government in some circumstances, such as when the dollar amount of transactions in a day exceeds a certain threshold. This would mean that people who store cryptocurrency in their own wallets would effectively be unable to transact anonymously with those who store their cryptocurrency with a custodial service.

FinCEN's language surrounding the use of "unhosted" wallets could be read to imply there is something unusual, or even nefarious, about wallets that are not "hosted," or that cryptocurrency is by default maintained by custodians. In reality, these independent stores of cryptocurrency are the fundamental provider of security and privacy for individual cryptocurrency users—just as people have long relied on cash for individual financial privacy and security.

IV. The Proposed Regulation Would Give the Government Access to Troves of Sensitive Data, Even Beyond What the Proposal Contemplates

The amount of sensitive data the government would be able to glean from its proposed new rule is vast, undercutting claims that the rule is narrow. The proposed regulation purports to require cryptocurrency transaction data to be provided to the government only when the amount of the transactions exceed a particular threshold. However, because of the nature of public blockchains, the regulation would actually result in the government gaining troves of data about cryptocurrency users far beyond what the regulation contemplates.

---

[6] 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.

[7] 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-censorship-paypal-makes-habit-deciding-what-users-can-read.

[8] Esther Addley and Jason Deans, *WikiLeaks Suspends Publishing to Fight Financial Blockade*, The Guardian (May 31, 2017), available at https://www.theguardian.com/media/2011/oct/24/wikileaks-suspends-publishing.

For some cryptocurrencies like Bitcoin, transaction data—including users' Bitcoin addresses—is permanently recorded on a public blockchain. For each Bitcoin transfer, the information that is publicly displayed includes the Bitcoin address of the sender and the receiver—an alphanumeric string akin to a username, which a user can use once or for multiple transactions. Bitcoin addresses are pseudonymous, not anonymous—and the Bitcoin blockchain is a publicly viewable ledger of all transactions between these addresses. That means that if you know the name of the user associated with a particular Bitcoin address, you can glean information about *all* of their Bitcoin transactions that use that address.

The proposed regulation requires that money service businesses collect identifying information associated with wallet addresses and report that information to the government for transactions over a certain threshold. But when the government learns the identity associated with a particular cryptocurrency address, it will also know the identity associated with *all* transactions for that cryptocurrency address (which are publicly viewable on the blockchain), even when the amounts of those transactions are far below the reporting threshold. While the identity associated with the counterparties to those other transactions may not always be known, the government's database may well also contain that information because of the breadth of the proposed regulation. This means that the proposed regulation would actually provide the government with access to a massive amount of data beyond just what the regulation purports to cover.

The government may imagine that collecting additional information about cryptocurrency users is not problematic in and of itself, and thus this implication of the proposed regulation is acceptable, but this could not be farther from the truth.

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 own files were recently exposed to the public, making it clear that FinCEN's security protocols are not adequate to prevent even large-scale leakage.[9] 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.[10] As just a few other examples, a hack of the Office of Personnel Management exposed over 22 million personnel records[11] and a breach of a voting records database led to the personal information of over 190 million Americans

[9] Noam Scheiber and Emily Flitter, *Banks Suspected Illegal Activity, but Processed Big Transactions Anyway*, New York Times (Sep. 20, 2020), available at https://www.nytimes.com/2020/09/20/business/fincen-banks-suspicious-activity-reports-buzzfeed.html.
[10] David E. Sanger et al., *Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit*, New York Times (Dec. 14, 2020), available at https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.
[11] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, Washington Post (July 9, 2015), available at https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

being published online.[12] 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.

V. The Proposed Regulation Violates the Fourth Amendment

The proposed regulation violates the Fourth Amendment's protections for individual privacy. Our society's understanding of individual privacy and the legal doctrines surrounding that privacy are evolving. 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."[13] In 1976, the Supreme Court pointed to the third-party doctrine in holding in *U.S. v. Miller*[14] 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."[15] 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

[12] Jim Finkle and Dustin Volz, *Database of 191 Million U.S. Voters Exposed on Internet: Researcher*, Reuters (Dec. 28, 2015), available at https://uk.reuters.com/article/us-usa-voters-breach-idUKKBN0UB1E020151229.
[13] *United States v. Jones*, 565 U.S. 400, 417 (Sotomayor, J. concurring).
[14] 425 U.S. 435 (1976).
[15] 416 U.S. 21, 78-79 (1974) (Powell, J. concurring).

government's misplaced reliance on the third-party doctrine. This includes: *U.S. v. Jones* (2012),[16] 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),[17] 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.*,[18] in which the Court held that police must obtain a warrant before accessing cell site location information from a cell phone company. EFF is heartened to see these 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. We believe this understanding of privacy can and should extend to our financial data. We urge FinCEN to heed the more nuanced understanding of privacy rights seen in modern court opinions, rather than anchoring its privacy thinking in precedents from a more analog time in America's history.

VI. The Proposed Regulation Must Demonstrate Compliance With International Privacy and Data Protection Principles

The expanded reach of the proposed regulation may 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,[19] as well as in the recent case law of the European Court of Human Rights concerning the Protection of Personal Data.

---

[16] 565 U.S. 400 (2012).
[17] 573 U.S. 373 (2014).
[18] No. 16-402, 585 U.S. ___ (2018).
[19] Necessary and Proportionate Coalition, *Global Legal Analysis* (May 2014), available at http://necessaryandproportionate.org/global-legal-analysis; Privacy International, *Guide to International*

The current proposal does not outline how this regulation would seek to resolve such potential conflicts of law between the United States and other jurisdictions. We urge FinCEN to 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.

VII. The Proposed Regulation Would Have Unintended Consequences for Blockchain Technology, Chilling Innovation

The proposed regulation would have unintended consequences for smart contracts and other decentralized technology with a wide range of lawful uses, and could chill blockchain innovation.

Under the proposed rules, money service businesses would have to collect certain identity information—such as names and physical addresses—about wallet users who transact with their customers. That requirement is problematic for several reasons: first, it presupposes that the wallets that their customers transact with are tied to particular humans; in reality, many such wallets will be part of an automated system with which the user transacts. Second, even when the counterparty to a transaction is a person, the proposed regulation would add friction to transactions, making it significantly more difficult for cryptocurrency users to interact with others who use a service subject to the regulation.

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

---

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.

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.[20]

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. Smart contract technology should not be broadly regulated by the Department of the Treasury; while FinCEN has a key role in this space, regulations should be carefully tailored—with input from the industry and experts—to avoid unintended consequences for a broad swath of emerging technologies. This proposed regulation in particular would have unintended consequences that could hinder smart contract development. The regulation's requirement that money service businesses collect identity information for wallets that are counterparties to their customers' transactions is impossible to comply with when the counterparty is not a person but rather part of a smart contract system.

This regulation could also have a serious impact on the development of 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

[20] We offer Audius not to draw attention to this particular application, but as one example of the many types of innovation we can expect to see in this space in the future.

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.

FinCEN should be extremely cautious about crafting regulation targeting "unhosted" wallets in order to avoid interfering with the growing ecosystem of smart contract technology, including decentralized exchanges. The proposed regulation would not only chill experimentation in a field that could have many potential benefits for consumers, but would also prevent American users and companies from participating when those systems are deployed in other jurisdictions.

VIII. The Process for This Rulemaking Is Unusual and Improper

In addition to EFF's concerns with the substance of this proposed regulation, EFF is deeply concerned with the unusual and improper process surrounding this rulemaking. The 15-day comment period is unusually short and coincides with the winter holiday. This abbreviated comment period will no doubt prevent many concerned experts and users from offering feedback on the proposed regulation's deficiencies. These regulations require at least the regular 60-day comment period, and also demand a far broader debate given the potential effects on civil liberties and innovation.

While the Notice of Proposed Rulemaking points to alleged "threats to United States national interests" to justify the abbreviated comment period, the NPRM does not explain what the threat is, how that threat might be exacerbated by a 60-day comment period, or how a 15-day comment period over the winter break might benefit national security. Rather, the abbreviated comment period appears to be a transparent attempt at imposing a midnight regulation before the end of this presidential administration. However this regulation is implemented, it will happen under the next administration. That administration should have the opportunity to engage with the public about this proposal and ultimately decide whether to implement it.

IX. Conclusion

EFF appreciates the opportunity to submit comments to FinCEN on its proposed regulations. Because of the proposed regulation's potential impact on the civil liberties interests of technology users and potential chilling effect on innovation across a broad range of technology sectors, we urge FinCEN not to implement this proposal as it stands. We also urge FinCEN to provide at least 60 days for comment in order to correct the serious abnormalities of this rulemaking process and to ensure that civil liberties experts, innovators, technology users, and other members of the public have an opportunity to voice their concerns about the potential impact of the proposal.

Respectfully submitted,

Marta Belcher
Special Counsel
Aaron Mackey
Staff Attorney
Danny O'Brien
Director of Strategy
Rainey Reitman
Chief Program Officer

Electronic Frontier Foundation

Responsible Sourcing of Data Enrichment Services

June 17, 2021

PARTNERSHIP ON AI

Table Of Contents

Acknowledgements

This white paper draws heavily on insights and input gathered during semi-structured interviews with members of the AI enrichment ecosystem conducted throughout 2020 as well as during a five-part workshop series held in the fall of 2020. The workshop series brought together more than 30 professionals from different areas of the data enrichment ecosystem, including representatives from data enrichment providers, researchers and product managers at AI companies, and leaders of civil society and labor organizations. We'd like to thank all of them for their engaged participation and for reviewing and providing valuable feedback on the drafts of this white paper.

We'd like to thank Elonnai Hickok for serving as the lead researcher on the project and Heather Gadonniex for her committed support and championship. This work would not be possible without the invaluable guidance, expertise, and generosity of Mary Gray. Many PAI staff members, current and former, contributed directly and indirectly to this work. In particular, Sonam Jindal is leading the project and served as the lead editor of the white paper, B Cavello led the workshop series, Katya Klinova oversaw the development of the project from its inception.

Participants of the Responsible Sourcing of Data Enrichment Services Workshop Series who contributed their expertise, insights, and suggestions include Aleli Alcala (Chief Operations & Sustainability Officer, Amara and PCF), Bama Athreya (Labor Rights Specialist), Olivia Blanchard (Researcher, Digital Future Society Think Tank), Jessica Custer (Manager, BSR), Bryan Dai (CEO, Daivergent), Orinola Gbadebo-Smith (Co-Founder & CEO, Hugo), Iva Gumnishka (Founder and CEO, Humans in the Loop), Dean Jansen (Executive Director, Participatory Culture Foundation), Kristen Itani Koue (Senior Impact Manager, Sama), Ivan Lee (CEO, Datasaur.ai), Milagros Miceli (TU Berlin/Weizenbaum Institute), Pamela Mishkin (Policy, OpenAI), Graeme Phillipson (Senior Project Engineer, BBC R&D), and Mark Sears (Founder & CEO, CloudFactory).

While individuals representing many of PAI's Partner organizations contributed text or suggestions to this document, it should not be read as representing the views of any specific member of the Partnership. Additionally, contributions from individuals do not necessarily reflect the views of their employers.

Please cite as following: *Partnership on AI, 2021. Responsible Sourcing of Data Enrichment Services. Available at: partnershiponai.org/responsible-sourcing.*

Executive Summary

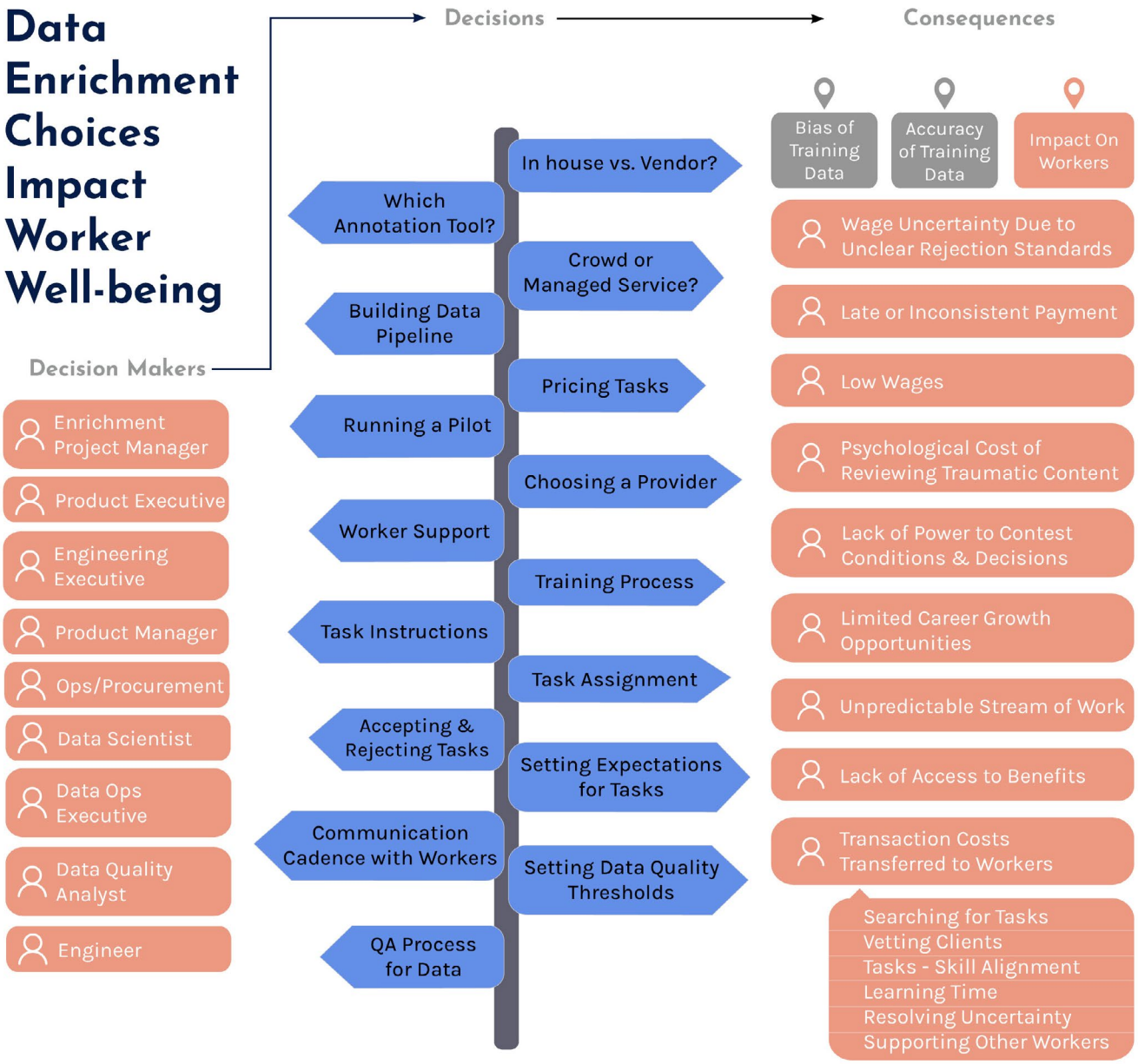
As AI becomes increasingly pervasive, there has been growing and warranted concern over the effects of this technology on society. To fully understand these effects, however, one must closely examine the AI development process itself, which impacts the world both directly and through the models it creates. This white paper 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.

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. Given that this process of labeling and enriching data inherently embeds human judgement and lived experiences into data, AI's intelligence is highly dependent on human intelligence. Despite the foundational role played by these data enrichment professionals, a growing body of research reveals the precarious working conditions these essential, but largely unseen, workers face.[1] There is, however, an opportunity to make a difference. The decisions AI developers make while procuring enriched data have a meaningful impact on the working conditions of data enrichment professionals. This paper focuses on how these decisions during the procurement process impact workers and proposes avenues for AI developers to meaningfully improve these working conditions.

This paper draws upon existing literature on the experience of data enrichment professionals and insights gathered from AI developers and key stakeholders through conversations and a series of workshops. Acknowledging the existing complexity and lack of standards around how to build equitable data supply chains, we aim to critically evaluate the impact of the industry's current practices on workers, explore practices the industry can adopt to improve worker well-being, and advance the discourse around the future of data enrichment work and the indispensable role it plays in AI development. While more work and research is needed, we have outlined key worker-oriented considerations that practitioners can use as a starting point to raise conversations with internal teams and vendors. Specifically, this paper covers worker-centric considerations for AI companies making decisions in: selecting data enrichment providers, running pilots, designing data enrichment tasks and writing instructions, assigning tasks, defining payment terms and pricing, establishing a communication cadence with workers, conducting quality assurance, and offboarding workers from a project.

Our intention with this paper is to aid the industry in accounting for well-being when making decisions about data enrichment and to set the stage for further conversations within and across AI organizations. Recognizing the critical role that data enrichment professionals play in building AI is imperative, both for ensuring that their work is fairly recognized and compensated and for understanding that the resulting models are a product of human intelligence. We hope this paper serves as a step forward, bringing us closer to a world where data enrichment professionals are recognized and rewarded by the industry for their central role in enabling AI advancement.

1 Gray, M.L and Suri. S. 2019. Ghost Work: How to Stop Silicon Valley From Building a New Global Underclass. Houghton Mifflin Harcourt. Google-Books-ID: 8AmXDwAAQBAJ


Data Enrichment Choices Impact Worker Well-being
Decision Makers
Enrichment Project Manager
Product Executive
Engineering Executive
Product Manager
Ops/Procurement
Data Scientist
Data Ops Executive
Data Quality Analyst
Engineer
Decisions
In house vs. Vendor?
Which Annotation Tool?
Crowd or Managed Service?
Building Data Pipeline
Pricing Tasks
Running a Pilot
Choosing a Provider
Worker Support
Training Process
Task Instructions
Task Assignment
Accepting & Rejecting Tasks
Setting Expectations for Tasks
Communication Cadence with Workers
Setting Data Quality Thresholds
QA Process for Data
Consequences
Bias of Training Data
Accuracy of Training Data
Impact On Workers
Wage Uncertainty Due to Unclear Rejection Standards
Late or Inconsistent Payment
Low Wages
Psychological Cost of Reviewing Traumatic Content
Lack of Power to Contest Conditions & Decisions
Limited Career Growth Opportunities
Unpredictable Stream of Work
Lack of Access to Benefits
Transaction Costs Transferred to Workers
Searching for Tasks
Vetting Clients
Tasks - Skill Alignment
Learning Time
Resolving Uncertainty
Supporting Other Workers

1. Introduction

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." [2]

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.[3] 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.[4] 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 will focus 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 Please see the Definitions section for a working definition of "data enrichment" work.

3 According to a Cognilytica report, the market for AI and machine learning preparation solutions has been estimated to grow to $1.2B by the end of 2023. For more information see: Data Engineering, Preparation, and Labeling for AI 2019. Cognilytica. January 31st 2019. Accessed September 10th 2020. https://www.cognilytica.com/2019/03/06/report-data-engineering-preparation-and-labeling-for-ai-2019/

4 Metz, Cade. A.I. Is Learning From Humans. Many Humans. The New York Times. August 16th 2019. Accessed August 12th 2020. https://www.nytimes.com/2019/08/16/technology/ai-humans.html

2. Methodology

This white paper draws heavily on existing research, media articles, international best practices, examples of company practice as found in company policy, and informal interviews with suppliers and clients of data enrichment work conducted by the Partnership on AI throughout 2020. The paper also draws heavily on comments and insights received during a five-week workshop series held in the fall of 2020, which brought together more than 30 professionals from different areas of the data enrichment ecosystem, including representatives from data enrichment providers, researchers and product managers at AI companies, and leaders of civil society and labor organizations.

The white paper recommendations are informed by:

- An analysis of practices and challenges that data enrichment service providers and their clients face, as identified through informal interviews with clients and providers in the ecosystem conducted throughout 2020;

- A review of challenges data enrichment workers face and the positive and negative impact on workers as a result of that data enrichment work, associated business models, and client practices as identified in existing research and literature;

- Regulations and guidelines covering business and human rights, supply chain and sourcing practices, and workers rights.

3. Definitions

Data enrichment work: Data curation for the purposes of machine learning model development that requires human judgment and intelligence. This can include data preparation, cleaning, labeling, and human review of algorithmic outputs, sometimes performed in real time. Examples of data enrichment work:

- Data preparation, annotation, cleaning, and validation:
    1. Intent recognition
    2. Sentiment tagging
    3. Image labeling
- Human review (sometimes referred to as "human in the loop"):
    1. Content moderation
    2. Validating low confidence algorithmic predictions
    3. Speech to text error correction

For the purposes of this white paper we refer to all these types of work as data enrichment work. The term "data enrichment" has been used by multiple companies in the industry to describe these services offered.[5] Other terms that have been used to refer to this work have included "data labelling," "data annotation," and "data curation."

Sourcing data enrichment work: A process that requires a number of steps including, but not limited to, defining the enrichment goal, choosing the enrichment provider, defining the enrichment tools, defining the technical requirements, writing instructions, ensuring that instructions make sense, setting worker hours, determining time spent on a particular task, communicating with enrichment workers, rejecting or accepting work, defining a project budget, determining workers' payment, checking work quality, and providing performance feedback.

Clients: For the purposes of this white paper we refer to professionals sourcing data enrichment work as "clients." People in a number of different roles can be involved in sourcing data enrichment work: See section 3.1, "Mapping the Ecosystem for Sourcing Data Enrichment Work," for more details.

Workers: For the purposes of this white paper we refer to individuals completing data enrichment as "workers." In doing so, we recognize the variety of employment statuses that can exist in the data enrichment industry, including independent contractors on self-service crowdsourcing platforms, subcontractors of data enrichment providers, and full-time employees.

3.1. Mapping the Ecosystem for Sourcing Data Enrichment Work

There are a number of decisions made by both clients and service providers over the course of sourcing data enrichment work. These decisions can involve coordination across a range of roles and can be done in-house, in collaboration with a service provider, in collaboration with a third-party partner like an academic institution, or in some combination of these. Based on feedback received during the Responsible Sourcing workshop series held by PAI, it is clear that there is a wide range of actors and choices involved in sourcing data enrichment work. Sourcing data enrichment work involves decisions around defining the work,

5 For example: imerit - https://imerit.net/, CloudFactory - https://www.cloudfactory.com/data-enrichment, Effect Force - https://force.effect.ai/enrichment/

selecting a service provider, and engaging with a service provider, which are made by a variety of stakeholders—from data scientists to company executives—across the hierarchy of an organization. This large range of stakeholders suggests a similarly large range of people that have the potential to step in to improve conditions for data enrichment workers.

4. Models of Engagement for Data Enrichment Services

Typically data enrichment work is offered via four different engagement models which often get combined. These models are:

1. **In-house data enrichment:** Clients may have an in-house team to carry out data enrichment work. Such a team might be staffed by full-time employees or contractors brought on to carry out data enrichment work. Contractors may be located on the premise of the client, but might not be treated as full-time employees. Clients may build their own tools or leverage existing annotation tools to manage their data enrichment work.

2. **Managed data enrichment service provider:** Clients may choose to work with managed data enrichment service providers that find, train, and manage workers to enrich data according to the clients' specifications. Managed service providers can work in a variety of configurations including employing an in-house team, working with a set of subcontractors, or even setting up tasks on crowdworking platforms on behalf of clients. Clients of managed service providers do not always have full visibility into the specific employment configurations used by service providers. Depending on the configuration of the service, workers can be full-time employees, consultants, or independent contractors. Managed service providers typically support their clients in developing and refining instructions and task design, monitoring quality, and determining the price for the work.

3. **Self-service crowdsourcing platform:** Crowdsourcing platforms act as an intermediary for task-based work, connecting clients and workers. Policies and practices vary platform to platform and clients can be faced with different tools and processes for developing and assigning tasks, ensuring quality, setting prices, making payments, and engaging with workers. Crowdsourcing platforms can have curated workforces or may be open for anyone to join. Some platforms provide clients with the ability to work with a "private crowd" specifically assembled for the duration of the project. Others provide application programming interfaces (APIs) which allow clients to customise the platform's core functionality to meet their unique needs. Workers on crowdsourcing platforms are typically considered to be independent contractors. This model can be considered as a sub-segment of what is often referred to as the "gig economy," or "platform economy."[6] While there are platforms that are fully dedicated to providing data enrichment work, tasks such as data labelling are also frequently done on platforms that offer other kinds of task-based work.

6 For example, Arne Kalleberg and Michael Dunn describe four categories of work platforms in the gig economy: crowdwork platforms, transportation platforms, delivery/home task platforms, and online freelance platforms. For more information see: Kalleberg, Arne, Dunn, Michael. Good Jobs, Bad Jobs in the Gig Economy. Perspectives on Work. 2016. Accessed September 5th 2020. http://michael-dunn.org/wp-content/uploads/2017/05/ALK-MD.-JQ-in-Gig-Economy.pdf

4. **Automated and synthetic:** Software can be used to carry out data enrichment work such as labelling, annotating, and tagging features in data sets and can be used to create new data sets that contain necessary attributes.[7] Automated and synthetic methods are typically used to supplement data enrichment work already being carried out by workers.

Each of the above models differ in terms of security requirements, cost, quality, flexibility, efficiency, and scalability. In-house services can provide the highest quality and security, but can be resource-intensive and less scalable.[8] As in other sectors,[9] an area of concern for managed services and crowdsourcing platforms could be unauthorized subcontracting.

5. Worker-Oriented Considerations for Clients

Upon identifying a need for data enrichment, it can be challenging to figure out the logistics of setting up a full data pipeline. There are numerous decisions to be made and often little guidance or established best practices. This section is meant to make it easier for those setting up data enrichment workflows to integrate workers' needs into the decision-making matrix from the outset. This section can also be used by companies with existing data enrichment workflows to critically analyze how their own practices may be impacting worker well-being and make changes. Collaborating with organizations that can bring in workers' perspectives and have a strong grounding in workers needs and rights can help achieve this and ensure that considerations of worker well-being are embedded within data enrichment workflows.

Drawing on the critical discourse around ethical supply chains and sourcing practices, labor rights, different dimensions of work via crowdsourcing platforms, and working conditions of data enrichment professionals, this section seeks to equip clients with key considerations necessary to make decisions that positively benefit workers. It also highlights how even decisions seemingly disconnected from workers can inadvertently impact them.

Upon identifying a need for data enrichment, it can be challenging to figure out the logistics of setting up a full data pipeline. There are numerous decisions to be made and often little guidance or established best practices. This section is meant to make it easier for those setting up data enrichment workflows to integrate workers' needs into the decision-making matrix from the outset. This section can also be used by companies with existing data enrichment workflows to critically analyze how their own practices may be impacting worker well-being and make changes. Collaborating with organizations that can bring in workers' perspectives and have a strong grounding in workers needs and rights can help achieve this and ensure that considerations of worker well-being are embedded within data enrichment workflows.

Once a client has determined the requirements of a data enrichment project, there are a series of steps and decisions that follow for selecting a service model and provider, defining the terms of engagement, and managing the entire data enrichment workflow. The rest of this section highlights choices made during the data enrichment process where clients should incorporate key worker-oriented considerations. As direct customers of enrichment services, clients' actions have a tangible impact on worker experience.

7 Krig, Scott. Ground Truth Data, Content, Metrics, and Analysis. Computer Vision Metrics. Apress. May 26th 2014. Accessed August 12th 2020. https://link.springer.com/chapter/10.1007/978-1-4302-5930-5_7.

8 Lee, Ivan. Data Labeling for Natural Language Processing. A Comprehensive Guide. datasaur.ai. September 42020. Accessed February 13th 2021. https://medium.com/datasaur/data-labeling-for-natural-language-processing-a-comprehensive-guide-741343fea20e

9 Deloitte. Responsible Supply Chain Tools: Understanding the Market Opportunity. April 2019. Accessed August 12th 2020.

As direct customers of enrichment services, clients' actions have a tangible impact on worker experience. By incorporating the below considerations into their decisions, clients have the ability to positively influence workers' livelihoods and well-being.

We will highlight conscious practices clients should incorporate into their decision making during the following points of the data enrichment sourcing process:

- Selecting a service provider
- Managing data enrichment workflows, including:
  a. Running a pilot
  b. Designing tasks, developing instructions, creating training materials, and setting timeframes
  c. Assigning tasks
  d. Defining payment terms and pricing
  e. Establishing communication cadence
  f. Assuring quality
  g. Closure and offboarding

The sections below explain how each of the above decision points impact worker experience and provide recommendations for how clients can promote better practices. We recognize project requirements often guide clients' decisions around selection and management of the data enrichment work (e.g. timeframe, scale, data security needs, and available budget). By specifically highlighting how these decisions impact labor conditions, we hope to empower clients with the tools they need to incorporate the consideration of worker well-being into the decision-making process.

5.1. Service Provider Selection

After a client decides that they will need data enrichment work for the development of their AI solution, they will need to choose a service model and likely a vendor or company to engage with. As noted in Models of Engagement for Data Enrichment Work, the most common models by which clients take on data enrichment work are in-house data enrichment, managed service, crowdsourcing platforms, automated software, or some combination of these. In addition to taking into account how different solutions may meet the company's objectives with respect to scale, cost, security, and quality, it is also important to take into consideration the impact on working conditions for data enrichment professionals. Annex 1: Crowdsourcing Platform Comparison lists a few existing resources that compare crowdsourcing platforms on criteria such as transparency of terms of service, commitment to fair wages, etc. However, these resources do not fully account for different models for sourcing data enrichment work. While it may be difficult to provide a comprehensive guide that accounts for the full range of engagement models, we intend to work towards addressing this gap by building off of company-specific commitments that are emerging.[10] We have identified nine worker-oriented considerations that can be used by clients to guide decisions around selecting a data enrichment service provider. To the extent possible, we have adapted these to apply broadly to different models of sourcing data enrichment work. The considerations include:

1. What commitments to labor standards, models of ethical sourcing, and social missions are in place?

2. What worker-oriented protections and considerations are incorporated within the terms of service, privacy and security policies, and redress mechanisms? How are workers' interests represented in these policies?

https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-about-deloitte-humanity-united-responsible-supply-chain-tools.pdf

10 For example, Appen has developed a "Crowd Code of Ethics" which includes a commitment to fair pay, inclusion, crowdvoice, privacy and confidentiality, communication, and well-being. For more information see: https://appen.com/crowd-wellness/

3. What benefits and support programs are in place for workers?

4. What information is available with respect to pricing models and base wages for workers?

5. What opportunities for recognition and reputation building are available to workers?

6. What work space, equipment, and forms of communication are available to workers?

7. What training is provided to workers and how is training time compensated?

8. What processes and mechanisms are in place to encourage diversity?

9. What policies and support structures are in place to address potential exposure to graphic or age-sensitive content?

Recognizing the differences between service models (i.e. managed service vs. crowdsourcing platform), we have explained how each of these considerations applies to various service models and have supported each consideration with an explanation of the implications for workers. The full list of considerations and explanations can be found in Annex 2: Considerations for Service Provider Selection.

5.2. Management of Data Enrichment Work

Clients undertake a series of steps related to the engagement and management of the data enrichment work. These include defining the enrichment tooling, defining technical requirements, designing enrichment tasks and writing instructions, ensuring instructions make sense to the workers, assigning tasks, setting payments and timeframes, rejecting or accepting work, checking quality, communicating with workers, and closing and offboarding of the project. While managed service providers may work alongside clients to manage some or all of these steps, clients directly using crowdsourcing platforms often manage these steps on their own. Various platforms offer differing levels of support, policies, processes, interfaces, and tooling for enrichment work. Management of workers and tasks can be partially or fully automated.[11] The below sections provide considerations for how clients can approach the various steps of managing data enrichment work and outline existing tools and guidance, with the aim of enabling positive outcomes for workers.

Running a Pilot

As with most product development, developing AI solutions is often an iterative process that requires flexibility. As a result, it can be difficult to set realistic expectations on timing and cost for a data enrichment project at the beginning. By running a pilot with a smaller subset of data prior to implementing a data enrichment project,[12] clients can establish a more realistic baseline for time and cost, refine task design,

11 There is a body of research that examines the use of algorithms for managing work on crowdsourcing platforms and the impact of the same on workers. For example, see: Aj, Wood, M. Graham, V, Lehdonvirta, I, Hjorth. Good Gig, Bad Gig: Autonomy and Algorithmic Control in the Global Gig Economy. Work, Employment & Society: a Journal of the British Sociological Association. August 8th 2018. Accessed September 12th 2020. https://europepmc.org/article/pmc/pmc6380453 and Lehdonvirta, Vili. Algorithms that Divide and Unite: Delocalisation, Identity and Collective Action in 'Microwork'. Chapter in Space, Place, and Global Digital Work. January 2016. Accessed September 22nd 2020. https://www.researchgate.net/publication/305365965_Algorithms_that_Divide_and_Unite_Delocalisation_Identity_and_Collective_Action_in_'Microwork'

12 https://playment.io/blog/refine-your-data-labeling-strategy-with-a-realistic-decision-framework

establish clear acceptance and rejection criteria for tasks, and assess impact of potential guidelines on workers.[13] More specifically, a pilot can help with:

- **Setting Timeframes:** During a pilot, clients can collect data and establish a baseline for the amount of time needed to complete all activities related to completing a task, including reading the instructions, reviewing examples, reviewing documentation, completing and submitting a task, and more. This can inform the final timeframe that is set for each task and the project.

- **Defining Per-Task Payment:** While there is additional complexity around defining the parameters of "per-task" work and what is included in a given "task," pilots can help companies develop baselines for how much time a task will realistically take for workers. The time required to complete a task is highly variable for different projects depending on the state of the data, amount of training necessary for workers, how long it takes workers to get used to a task, difficulty of the task, whether the task will require consulting outside sources, and more. In order to estimate the amount of time necessary for a given task, clients can deliberately evaluate the distribution of amounts of time it took workers to complete a task during a pilot. Using this distribution and a living wage base (usually based on hourly living wage for a given location), clients can calculate what would be a reasonable per-task payment. When such benchmarks are available, it is a good practice to compare that number to fair payments for similar tasks performed at larger scale.

- **Writing Good Instructions, Designing Tasks, and Ensuring Tool Usability:** During a pilot, clients can "test" their instructions, worker experience of completing the tasks based on task design, and usability of the enrichment tool. They can do this by collecting direct feedback from workers through surveys, regular check-in sessions, and worker interviews. This feedback can inform any necessary improvements before scaling the enrichment process.

Similar to any product pilot, it is important to follow research best practices to limit skewed results. That being said, being mindful of how a data enrichment project is being set up and running a pilot to gather workers' feedback can meaningfully help clients to set realistic timeframes, improve task instructions and tools, improve worker experience, and establish a fair price for each task.

Designing Tasks, Developing Instructions, Creating Training Materials, and Setting Timeframes

Designing tasks, developing instructions, developing training materials, outlining performance expectations, and establishing clear timeframes are essential components of setting up a data enrichment project. In most cases, clients are involved in each of these decisions which have a meaningful influence on both the workers' experience with fulfilling the tasks and on the quality of enriched data. If the client has engaged with a managed service provider, they may work together to develop the project parameters, instructions, training materials, etc. In these circumstances, clients may stipulate the tool or platform that the managed service should use or defer to the managed service's preferred tools.

13 For example, researchers at Stanford University have looked to improve the quality of task designs through "prototype tasks," a strategy that requires all new tasks to be run through a rapid sample run where workers have the ability to provide feedback on the task design. The research found that running a prototype with a small sample of workers resulted in better outcomes for both clients and workers. For more information see: Gaikwad, Snehalkumar. Chhibber, Nalin. Prototype Tasks: Improving Crowdsourcing Results through Rapid, Iterative Task Design. Stanford Crowd Research Collective. 2017. Accessed September 5th 2020. https://arxiv.org/pdf/1707.05645.pdf. Running a pilot to understand what would be a proportionate payment has also been recommended by researchers. See: Papoutsaki, Alexandra, Guo Hua, Kakavouli Metaxa, Danae. Crowdsourcing from Scratch: A Pragmatic Experiment in Data Collection by Novice Requesters. Proceedings, the Third AAAI Conference on Human Computation and CrowdSourcing. 2015. Accessed September 5th 2020. https://www.aaai.org/ocs/index.php/HCOMP/HCOMP15/paper/viewFile/11582/11436

Though crafting effective instructions can be challenging, investing in this process is critical. Taking the time to translate data enrichment needs into clear and concise instructions can save time in the long run by creating less confusion around guidelines and therefore less back-and-forth when executed tasks do not meet the necessary standards. By investing up front in explicit instructions with clearly communicated expectations, clients can decrease the chances of having to redo work, thereby making it more likely to meet budgets and timelines. As stated above, there is value in testing these instructions with workers during a pilot or in early feedback sessions with a smaller subset of workers. Intentionally prioritizing this process can not only save time and money, but positively shape worker experience. In addition to incorrect and delayed work for a project, research has highlighted that unclear instructions can impact workers ability to succeed[14] and can result in multiple iterations of a task, rejected and uncompensated work, or tasks that timeout.[15] On crowdsourcing platforms, multiple iterations and rejected work have a significant impact on a worker's ratings and can result in nonpayment for a task depending on how the platform is designed. Penalizing a worker's rating because they did not meet vaguely specified expectations can unfairly preclude them from getting future tasks. This places an unreasonable burden on workers when instructions are not clear and threatens their source of income. Furthermore, unclear instructions on crowdsourcing platforms create a situation where even workers who are putting in their best effort and investing time in completing tasks may have their work rejected and unpaid.

There is a body of research that has examined the challenge of task design and writing instructions on crowdsourcing platforms and has sought to develop solutions. Some companies have also published guidance on how to develop effective instructions for data enrichment work. These resources can be found in Annex 1: Task Design and Writing Instructions. Here, we highlight a few practices that can improve outcomes for workers:

Designing Tasks and Developing Instructions:

1. Define clear and consistent rules for what constitutes a well-executed task. Test them internally, as well as with data enrichment workers prior to implementing a task. Ensure continuous communication with workers if questions or issues arise.

2. Incorporate worker feedback into the instructions, particularly with respect to any unclear aspects of the tasks. This is important for both improving processes and empowering workers.

3. Keep in mind the audience when crafting instructions. Depending on the project, the team crafting instructions may have more extensive domain knowledge than the workers conducting the data enrichment work under tight timelines. Make sure that instructions provide enough context to enable workers to complete the task in the expected amount of time. As addressed earlier, testing the instructions with the workers can help to ensure their perspectives and questions are incorporated into the final instructions. Providing examples of correct and incorrect work can also go a long way in establishing clear expectations for workers.

14 Gadiraju, Ujwal, Yang, Jie, Bozzon, Alessandro. Clarity Is a Worthwhile Quality: On the Role of Task Clarity in Microtask Crowdsourcing. HT'7: Proceedings of the 28th ACM Conference on Hypertext and Social Media. July 2017. Accessed September 5th 2020. https://doi.org/10.1145/3078714.3078715

15 Semuels, Alana. The Internet Is Enabling a New Kind of Poorly Paid Hell. The Atlantic. January 23rd, 2018. Accessed September 5th 2020. https://www.theatlantic.com/business/archive/2018/01/amazon-mechanical-turk/551192/

4. To the extent possible, communicate the purpose of a task and how it connects to a larger project or objective.[16]

5. Ensure that consent forms and confidentiality agreements provide workers with the necessary context on how the enrichment work results will be used.[17]

6. Ensure that tasks are designed with the tool in mind in order to produce a clear and intuitive user experience. Additionally, ensure that instructions address how to navigate and use the tool to complete tasks efficiently and how to address any technical difficulties that may arise.

Developing Training Materials:

7. Analyze what type of background knowledge and training is needed in order to effectively complete the relevant tasks. Design and provide any necessary training to workers which will make the work easier for them and improve the quality of work.[18] Ensure that the training time is compensated.

Setting Timeframes:

8. When setting a timeframe, take into consideration the time needed to go through any preparatory work, complete the tasks themselves, and review work prior to submission. Preparatory work may involve reviewing instructions, reviewing consent forms and other associated documentation, and going through any required training.[19] Timeframes should also account for the amount of time it may take for workers to get acquainted with the user flow necessary to complete the task and some buffer time to address potential technical issues. One way to approach this would be to collect more granular data during the pilot to establish a baseline that takes these factors into account. In suggesting this, we recommend working closely with the workers during the pilot to get an accurate accounting of how much time was needed for the pre-task, task, and post-task activities. Another way may be to add a generous buffer to the slowest time from your pilot results. To the extent possible, clients should verify if the initial time estimates to complete a task were accurate and use this information to make adjustments.

9. If the workers on your project are not exclusively working for your team, design tasks and timeframes in a way that allows workers and contributors flexibility in how and when they complete a task so they can plan for their other work obligations.[20]

16 Research has explored different ways that training can be provided to workers on crowdsourcing platforms. Among other things, the research found that offering feedback and the purpose of a task positively impacted worker motivation. For more information see: Dontcheva, Mira, Morris, Robert, Brandt, Joel, Gerber, Elizabeth. Combining Crowdsourcing and Learning to Improve Engagement and Performance. CHI. 2014. Accessed September 10th 2020. https://affect.media.mit.edu/pdfs/14.Dontcheva-Morris-Gerber-Brandt-CHI.pdf

17 This has been recommended in guidelines on the use of crowdsourcing platforms from a number of Universities. For example see: https://www.umass.edu/research/guidance/mturk-guidance

18 For example, research has found that providing training to workers when necessary has been found to be an effective method of quality assurance. For more information see: https://arxiv.org/pdf/1801.02546.pdf

19 This approach has been recommended by the University of Waterloo in guidance on the use of crowdsourcing platforms. For more information see: https://uwaterloo.ca/research/office-research-ethics/research-human-participants/pre-submission-and-training/use-crowdsourcing-services

20 Yin, Ming. Suri, Siddharth, Gray, M.L. Running Out of Time: The Impact and Value of Flexibility in On-Demand Crowdwork. CHI'18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. April 2018. Accessed September 5th 2020. https://dl.acm.org/doi/abs/10.1145/3173574.3174004

Assigning Tasks

Depending on the engagement models, the mechanisms by which tasks are assigned to workers may differ. Clients and managed service providers can be more directly involved with assignments when working with contractors or full-time employees. Crowdsourcing platforms typically provide recommendations and filters to support task assignment based on parameters like skill set, area of expertise, qualifications, rating, performance statistics, work histories, test scores, rejection rates and others.[21] These matching algorithms have been controversial and raised questions about fairness, the bias that these systems may inadvertently bring in, the impact of these on worker autonomy, and the way in which workers may unfairly lose access to platforms they rely on to make a living.[22] It is important that clients exercise caution and incorporate a deliberate consideration of worker well-being when using automated matching algorithms and filters.

Finding the right worker for a task is important and can be challenging. As researchers have noted, a mismatch between the skills and knowledge required for a task can result in delayed projects, inaccurate work, and rejected work.[23] Rejected work is particularly costly to workers who may have committed to a task before being shown the full details: not only do workers usually get penalized in their ratings for rejected work, they may not get paid for the critical time they have already invested in completing the task to the best of their ability. In other employment models, employers invest significant energy in finding the right fit between workers and skills required. When an imperfect algorithm is used for matching, the transaction costs of finding the right fit usually falls on workers. Researchers have explored ways in which platforms can improve matching tasks and workers by taking into consideration nuanced characteristics of both.[24] Other work has explored solutions that can help clients navigate worker selection on crowdsourcing platforms by bringing together different dimensions related to pricing, task difficulty, and worker skill.[25]

Considerations related to task assignment that can improve the outcome for workers and the quality of data include:

- **Redundancy:** To improve enriched data accuracy as well as reduce biases, consider assigning multiple workers to the same tasks to confirm the results are the same.

- **Workforce Consistency:** Given the importance of consistency across related datasets, the level of skill that is needed for nuanced complex data enrichment work, and the value of strong relationships in ensuring smooth work processes, clients should consider engaging with the same workers on a crowdsourcing platform or team at a managed service provider. This can also allow workers to build reputations, relationships, and skill sets which can all be leveraged to find opportunities in the future. Engaging with the same workers can also help ensure high-quality enriched datasets.[26]

21 https://www.ischool.utexas.edu/~ml/papers/donna-iconf15.pdf

22 https://dl.acm.org/doi/abs/10.5555/3398761.3398923, https://journals.aom.org/doi/10.5465/annals.2018.0174, https://journals.sagepub.com/doi/full/10.1177/0950017018785616

23 For example, research has explored the creation of human-oriented frameworks for crowdsourcing towards addressing issues like unfair compensation, incompatible task assignments, and unintended amplification of human biases. For more information see: Barbosa, Nata, Chen, Monchu. Rehumanized Crowdsourcing: A Labeling Framework Addressing Bias and Ethics in Machine Learning. In CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019. Accessed September 10th 2020. https://www.natabarbosa.com/chi_rehumanized_crowdsourcing.pdf

24 Schnitzer, Steffen, Rensing, Christoph. Demands on Task Recommendation in Crowdsourcing Platforms - the Worker's Perspective. CrowdRec. September 19th 2015. Accessed September 5th 2020. https://www.semanticscholar.org/paper/Demands-on-task-recommendation-in-crowdsourcing-Schnitzer-Rensing/e411b1e635698a47a6e82acf2e67718780f0579c

25 Rajpal, Shreya, Goel, Karan, Mausam. POMDP-Based Worker Pool Selection for Crowdsourcing. Proceedings of the 32nd International Conference on Machine Learning. Lille France, 2015, Accessed September 10th 2020. http://www.crowdml.cc/icml2015/papers/CrowdML-Paper19.pdf

26 Daniel, Florian, Kucherbaev, Pavel, Cappiello, Cinzia, Benatalla, Boualem, Allahbakhsh, Mohammad. Quality Control in Crowdsourcing: A Survey of Quality Attributes Assessment Techniques and Assurance Actions. ACM Comput. Surv. Article 7 January 2018. Accessed September 10th 2020. https://arxiv.org/pdf/1801.02546.pdf

- **Attention to Diversity:** Given the subjective nature of classifying and labeling data, it is important to pay attention to the diversity of data enrichment workers. A lack of diversity could be a source of bias in the labeled dataset.

- **Mindful Screening Criteria:** When selecting how to screen workers, consider the impact that each applied filter may have on the workers, and if the filter accurately captures the skills or qualities needed. For example, research has recommended that workers should not be screened based on non-payment rates as non-payment does not necessarily reflect quality and that workers should not be penalized (through poor ratings or other actions) for refusing to accept a task.[27]

Defining Payment Terms and Pricing

Clients set or negotiate payment for data enrichment work. There are four predominant pricing models for data enrichment services:

- **Per Task:** This is a common payment model on crowdsourcing platforms. If data enrichment workers are being paid by the task, the price per task is often set by the client, sometimes with input from the service or platform they are working with[28] or through a bidding process facilitated by the platform.[29] Given the international makeup of workers on crowdsourcing platforms, a bidding process in which workers bid for tasks drives prices per task down. Adding to worker precarity, many platforms allow clients to reject work without payment after workers have already completed the task.[30] There are no standard rules or guidelines to protect workers from unpredictable payment rates.

- **Per Hour:** If workers are being paid by the hour, they are typically paid for the total amount of time spent completing the necessary tasks. Time can be tracked either by the tool being used or through manual time-recording through timesheets. If a tool is recording time, how that time is measured is critical to ensuring that workers are being paid fairly.

- **Per Tier of Service:** Clients may also pay managed service providers a fixed fee for a given tier of service and use per task payment if there is a need to go beyond what is included in the base price. Under this service model, the managed service provider would typically determine the workers' wages.

- **Flat Fee:** Clients may also pay managed service providers a flat amount per project delivered which is negotiated specifically for each individual project.

27 Worker evaluations and ratings should not be based on non-payment rates and workers should be given reasons for any negative ratings. For more information see: Berg, Janine, Furrer, Marianne, Harmon, Ellie, Rani, Uma, Silberman, Six. Digital Labour Platforms and the Future of Work. International Labour Organization. 2018. Accessed September 10th 2020. https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_645337.pdfhttps://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_645337.pdf

28 For example, research that undertook a comparison of platforms has noted that platforms such as LeadGenius automatically set the price per task based on estimations of completed time, effort, and local hourly wages. The prices can be adjusted if the task takes longer than estimated. For more information see: Vakharia, Donna, Lease, Matthew. Beyond Mechanical Turk: An Analysis of Paid Crowd Work Platforms. iConference 2015. Accessed September 10th 2020. https://www.ischool.utexas.edu/~ml/papers/donna-iconf15.pdf

29 Royer, Alexandrine. The Urgent Need for Regulating Global Ghost Work. Brookings, Brookings, 9 Feb. 2021, Accessed May 18, 2021 https://www.brookings.edu/techstream/the-urgent-need-for-regulating-global-ghost-work/

30 Pury, Cynthia, Brawley, Alice. Work Experiences on MTurk: Job Satisfaction, Turnover, and Information Sharing. Computers in Human Behavior 54 p. 531-546, September 11th 2015. Accessed September 5th 2020. http://crowdsourcing-class.org/readings/downloads/ethics/mturk-job-satisfaction.pdf

Independent of the pricing model used, running a pilot and collecting data about the amount of time it takes workers to complete all activities related to a given task is critical to estimating how a task should be priced. The amount of time it takes to do the task and any necessary pre- and post-completion activities should all be used to estimate a worker's hourly compensation and accurately assess if the per hour total compensation is fair.

When using a crowdsourcing platform directly or working with a managed service that uses a crowdsourcing platform, it is critical to be attentive to how the platform structures its payments with workers. Clients engaging with crowdsourcing platforms can make a difference in workers' lives by watching out for the following:

- **Unreasonably Low-Priced Tasks:** A wide range of tasks and task types, a lack of standards for how tasks should be priced, and platform designs which force workers to bid for tasks all contribute to tasks being priced down. In particular, as mentioned above, when platforms force workers to compete for tasks with workers from around the world, there is a race to the bottom. Without the client's active consideration, workers may end up getting paid unreasonably low amounts. When choosing a platform to work with or working with a managed service using a crowdsourcing platform, clients should make sure they have the ability to pay workers a fair amount for their contributions. The next section covers ways to calculate this.

- **Lost Wages:** Another important payment term consideration when choosing a platform or vendor is how the platform handles accepting and rejecting completed tasks. While investing in a pilot that helps craft effective instructions and training materials can limit rejections later in the project, some work may still need to get rejected occasionally. If completed work is rejected without explanation and the worker's ratings go down, this can make it harder for them to get work later, result in lost wages for the work they have already put in, and can create a power imbalance if workers do not have meaningful avenues for redress.[31] Some of this can be mitigated by ensuring that the crowdsourcing platform being used provides workers with transparency over why a task is rejected and workers have the ability to contest rejected tasks. Furthermore, the impact of rejections on lost pay can be decreased by reviewing work promptly and providing fair and detailed justifications for rejections, so workers can learn from the client's acceptance criteria and identify early on if their skill set does not match the needs of the project and step down before investing too much time. Clients should still pay for rejected work if the rejection occurred for reasons outside of the worker's control.

- **Non-Monetary Payments:** Clients should ensure that the service or crowdsourcing platform they use is paying workers in cash as opposed to vouchers or rewards. Furthermore, it is worth asking the platform or managed service about their payment cadence to ensure they are regularly paying their workers.

- **Additional and Hidden Costs Borne by Workers:** In the absence of a formal management team, many of the functions that a "traditional" employer usually takes on as a part of managing their workforce come to land on workers' shoulders.[32] This is particularly true of crowdsourcing platforms. Workers take on the costs associated with tracking their own progress, searching for tasks, vetting clients, learning how to do tasks, resolving uncertainty when there is no one to answer questions, and oftentimes take on equipment costs.

31 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons from a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

32 Caitlin Lustig, Sean Rintel, Liane Scult, and Siddharth Suri. 2020. Stuck in the middle with you: The transaction costs of corporate employees hiring freelancers. Proc. ACM Hum.-Comput. Interact. 4,CSCW1, Article 37 (May 2020), 28 pages. https://doi.org/10.1145/3392842

Furthermore, they do not have access to benefits, pay local taxes, and often pay a transaction fee per task to the platform[33] or an overarching fee to access the platform.[34] When choosing a crowdsourcing platform to use, either directly or through a managed service, clients should evaluate the additional, uncovered costs workers bear on that platform and consider how the pricing strategy should reflect those additional costs.

As data enrichment becomes an increasingly common job,[35] it is crucial to address the low wages that characterize this sector. Clients have reported the challenges associated with identifying fair prices for data enrichment.[36] For crowdsourcing platforms, many best practices have highlighted the importance of paying at least a minimum wage in a jurisdiction (of the employer and employee), a fair wage, or a living wage.[37] Other solutions have explored the possibility of clients committing to a "wage pledge" to pay a minimum or living wage.[38] While the global labor market is increasingly complex, below is a summary of a few approaches clients can take to estimate a fair price for this labor.

- **Calculate and Pay at Least a Living Wage:** When working with a managed service provider, clients can demand transparency in the wage structure and ensure contracts with workers include a guaranteed living wage or at least the local minimum wage. There are a number of resources that can be used to calculate a living wage which are listed in Annex 1: Calculating a Living and Minimum Wage. When using these tools or setting a price, it is important to recognize the difference between a living wage (amount an individual needs to cover basic costs) and the minimum wage (legal minimum pay per hour), to consider where workers are located and living costs associated with the location, and to critically analyze the tool's inputs, how the information it uses was obtained, and how frequently it is updated, if at all.

- **Account for Additional Costs:** When relevant (especially when using crowdsourcing platforms), account for costs that workers may bear including time spent searching for tasks, time spent training and learning the parameters of a task, time spent reviewing task samples, platform fees workers may pay to access the platform, local taxes, equipment costs, and cost of basic benefits, such as healthcare and sick leave. In order to account for these additional costs, research suggests offering individuals categorized as self-employed a multiple of the minimum wage based on the worker's location or a multiple of the median local wage earned by employed individuals.[39] Recognizing that it can be challenging for clients to know the location of a worker, it can be useful for clients to use the maximum minimum wage for OECD and non-OECD countries.[40]

33 On Freelancer, for example, the platform takes a 3% cut from employers and a 10% cut from freelancers. For more information see: Freelancer Fees and Charges. Accessed September 5th 2020. https://www.freelancer.com/feesandcharges/#

34 For example, according to Fair Crowd Work, CrowdFlower charges $1,500 p/m for access to the platform. For more information see: Fair Crowd Work. CrowdFlower. Accessed September 5th 2020. http://faircrowd.work/platform/crowdflower/?ertthndxbcvs=yes

35 Silberman, M.S, Tomlinson, B, LaPlante, R, Ross. J, Irani. L, Zaldivar, A. Responsible Research with Crowds: Pay Crowdworkers at Least Minimum Wage. Communications of the ACM, March 2018, Vol, 61. No. 3. Accessed September 10th 2020. https://cacm.acm.org/magazines/2018/3/225476-responsible-research-with-crowds/fulltext

36 Caitlin Lustig, Sean Rintel, Liane Scult, and Siddharth Suri. 2020. Stuck in the Middle with You: The Transaction Costs of Corporate Employees Hiring Freelancers. Proc. ACM Hum.-Comput. Interact. 4, CSCW1, Article 37 (May 2020), 28 pages. https://doi.org/10.1145/3392842

37 See table comparing crowdsourcing principles and best practices in Annex 3.

38 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons From a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

39 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons From a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

40 Wage data for OECD countries is available at: https://stats.oecd.org/Index.aspx?DataSetCode=RMW

- **Leverage Data on Similar Tasks:** While pilots can help refine task pricing, referring to similar tasks in the past can also inform initial estimations.[41] That being said, prices should be adjusted if workers or data suggest that a task is taking more time than initially expected. If this is discovered after the fact, clients can compensate workers with bonuses.[42] Prices should also be adjusted based on difficulty of task.[43]

- **Track Task Completion Time:** Clients should confirm whether the actual completion times per task match the initial estimate. Depending on the data enrichment tool, this can be completed via the tool or can be ascertained via random sampling. The results can be used to offer a wage adjustment to workers and inform future iterations of the project.

- **Compensate for Changes That Occur on the Client Side:** Pay workers for lost time if there were workflow problems due to a lapse on the client's side, due to changes in the instructions or the scope of work, or unforeseen technical issues on the client or platform side.[44]

Establishing Communication Cadence

Clear communication is critical to ensuring that workers have the information they need to effectively and efficiently complete tasks. Research has shown miscommunication as an area of frustration for both workers and clients.[45] Having clear communication can positively impact worker experience, decrease the total amount of time to resolve uncertainties, and mitigate the risk of lost pay or missed deadlines due to misalignment. Depending on the engagement model, the communication methods and responsibilities may differ. Regardless of who is carrying out the communication, it is important to make sure there is an established process to communicate task assignments, training procedures, expectations around acceptable tasks, how to resolve uncertainty, and who to reach out to if any problems arise.

Communication practices that clients can use to improve the outcomes for workers include:

- Seek out feedback on communication from workers and make necessary adjustments. If you are using a pilot, ensure that the communication procedures and materials intended to be used during the project are also tested during the pilot. Another way to test communication procedures may be to have a targeted feedback session with a representative group of workers before widespread dissemination of communication materials and procedures. Getting this feedback earlier on can save time in the long run as it will help avoid misalignment.

41 This approach was suggested by the University of Waterloo in guidance on the use of crowdsourcing services for research. For more information see: University of Waterloo. Use of Crowdsourcing Services. Accessed September 5th 2020. https://uwaterloo.ca/research/office-research-ethics/research-human-participants/pre-submission-and-training/use-crowdsourcing-services

42 M. S. Silberman, B. Tomlinson, R. LaPlante, J. Ross, L. Irani, A. Zaldivar. Responsible Research With Crowds: Pay Crowdworkers at Least Minimum Wage. Communications of the ACM, March 2018, Vol. 61 No. 3. Accessed September 5th 2020. https://cacm.acm.org/magazines/2018/3/225476-responsible-research-with-crowds/fulltext

43 This approach was recommended in guidance to MIT researchers. For more information see: https://couhes.mit.edu/guidelines/couhes-policy-using-amazons-mechanical-turk

44 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons From a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

45 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons From a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf and Irani, Lilly, Silberman, M. Six. Turkopticon: Interrupting Worker Invisibility in Amazon Mechanical Turk. CHI 2013: Changing Perspectives, Paris, France. Accessed September 10th 2020. http://crowdsourcing-class.org/readings/downloads/ethics/turkopticon.pdf

- Use services that allow for clear communication with workers. When working with any service, particularly if a crowdsourcing platform is involved, consider which mechanisms are available to facilitate communication between workers and those overseeing the data enrichment process (either from the client or vendor side).

- Clarify expectations around communication prior to the start of the project and ensure workers know how to resolve uncertainty or who to reach out to should any issues arise. Additionally, make sure you have procedures in place to provide a quick turnaround for workers regarding any questions or concerns.[46]

- Provide early and consistent feedback. Establish regular milestones and checkpoints to review work and provide feedback to ensure that workers are aligned with the project's expectations. Regular feedback allows workers to make adjustments early on and help avoid project delays or extra costs arising from having to redo work.[47]

- Establish clear mechanisms for workers to contest rejections if they have reason to believe their work should not have been rejected. As mentioned earlier, providing feedback around when work meets or does not meet the acceptance criteria can allow workers to resolve issues earlier and make sure they are aligned with the project's guidelines. In addition to making sure that the acceptance and rejection process is accurate and fair, allowing workers to contest rejections can improve the overall quality of the data and provide workers with an avenue to recover ratings or lost wages.

- Build trust with workers by identifying yourself or the company you represent in the task name or description.[48]

Quality Assurance

As a critical input into AI models, the enriched data needs to be of a high quality. Once tasks are complete, clients or managed service providers typically undertake a final evaluation of the work and accept, reject, or request modifications. Evaluating the quality of enriched data can be challenging and raises questions about how to identify and handle inaccurate data, how to assess biased data, and how to handle payment for data that may not meet the necessary standards.

While setting clear expectations prior to the start of the project can mitigate some of the quality risks, it is also important to design the quality assurance process with workers in mind. Depending on the engagement model, the quality assurance process may look different. While managed service providers often take on an active role in supporting clients with conducting quality assurance, crowdsourcing platforms vary in terms of the support and mechanisms they provide.

46 For example, guidance for MIT researchers recommends that requesters respond to emails from workers within seven working days. For more information see: https://couhes.mit.edu/guidelines/couhes-policy-using-amazons-mechanical-turk

47 Papoutsaki, Alexandra, Hua Guo, Kakavouli, Danai, Gramazio, Connor, Rasley, Jeff, Xie, Wenting, Wang, Guan, Huang, Jeff. Crowdsourcing from Scratch: A Pragmatic Experiment in Data Collection by Novice Requesters. Proceedings, the Third AAAI Conference on Human Computation and Crowdsourcing. 2015. Accessed September 10th 2020. https://www.aaai.org/ocs/index.php/HCOMP/HCOMP15/paper/viewFile/11582/11436 and Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons From a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

48 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons From a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

There are many resources that explore different methods for quality assurance on crowdsourcing platforms. A few common methods include assigning test tasks to workers, tracking historical accuracy,[49] having workers go through training projects, and having multiple workers do the same tasks and reviewing tasks with disagreements.[50] Some of these approaches can be time-intensive and difficult to scale. Quality is highly dependent on a number of factors including the working conditions of data enrichment professionals, the quality of training provided to workers, the way tasks are designed, and the processes and mechanisms established by a particular platform.[51] It is worth calling out that some tasks require subjective judgement and can be labeled differently depending on the background of the workers and some tasks may require workers with a specific background or skill set. Being able to recruit a worker base with the specialized knowledge and relevant diverse backgrounds to complete tasks can determine the quality of the enriched dataset. Resources that dive into best practices around establishing quality assurance practices are further outlined in Annex 1: Quality Assurance.

In addition to influencing dataset accuracy and bias, quality assurance practices also have implications for workers. On a crowdsourcing platform, clients exercise their discretion in rejecting work they find to be inaccurate. For workers, this can result in unpaid labor, lower ratings, and lack of access to future work.[52]

Worker-minded practices to consider when establishing a quality assurance routine include:

- Ensure that the raw, unenriched data is of a high quality so it is easy to decipher for workers. This will result in higher quality enrichment and less inaccuracies.
- Clearly communicate acceptance and rejection criteria to workers prior to the start of the enrichment project.[53] Clarify how quality will be measured ahead of time in order to ensure that expectations are clear to all parties involved.
- Provide workers with examples of correct and incorrect work. This will also help workers familiarize themselves with the project's expectations.
- Provide workers with an opportunity to complete a sample of the work either in a test environment or a test project and confirm its accuracy prior to the start of the project.
- Provide mechanisms for workers to correct work upon receiving early feedback.[54] This will minimize the overall quantity of incorrect work done.

49 Barbosa, Nata, Chen, Monchu. Rehumanized Crowdsourcing: A Labeling Framework Addressing Bias and Ethics in Machine Learning. In CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK. ACM, New York, NY, USA. https://www.natabarbosa.com/chi_rehumanized_crowdsourcing.pdf

50 https://dsg.tuwien.ac.at/Staff/sd/papers/Zeitschriftenartikel%20-%20Quality%20Control%20SD%202013.pdf

51 https://arxiv.org/pdf/1801.02546.pdf

52 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons From a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf and Silberman, M.S ,Tomlinson, B, Laplante, R, Ross, J, Irani, L, Zaldivar, A. Responsible Research with Crowds: Pay Crowds: Pay Crowd Workers At Least Minimum Wage. Communications of the ACM. March 2018. Vol. 61, No. 3. Accessed September 10th 2020. Available at: https://cacm.acm.org/magazines/2018/3/225476-responsible-research-with-crowds/fulltext

53 This approach was recommended to researchers at Berkeley. For more information see: https://cphs.berkeley.edu/mechanicalturk.pdf

54 McInnis, Brian, Cosley, Dan, Nam, Chaebong. Taking a HIT: Designing around Rejection, Mistrust, Risk, and Workers' Experiences in Amazon Mechanical Turk. CHI'16: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. May 2016. Accessed September 5th 2020. https://doi.org/10.1145/2858036.2858539

- Ensure that workers have enough time to complete a given task and are paid appropriately for their time so they do not feel pressured to do tasks too quickly.

- If work is rejected for a reason not connected to quality, this should be clearly indicated. In these circumstances, make sure workers' ratings are not negatively impacted.

- If work is rejected and not compensated, include an explanation of why and provide a commitment to the worker that the work will not be used.[55]

- If a negative review is given to a worker, the reasons should be fully supported and communicated to the worker.[56]

Closure and Offboarding

It is important that workers are recognized and have the ability to provide feedback as part of the closure and offboarding process. These steps can help to bring recognition, power, and voice to workers.

Practices that can improve the outcome for workers during project offboarding include:

- Actively seek feedback from workers in order to make improvements in the future.[57]

- Recognize workers' contributions in context of the larger project. This will allow workers to build a reputation and portfolio of work which can help them develop their careers as data enrichment professionals. Recognizing the central role played by these professionals also helps push the industry towards greater transparency around the AI development process, which is critical to treating these workers with the respect they deserve and ensuring that their work is not hidden.

55 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons From a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

56 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons From a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

57 For example, guidance for researchers from the University of Massachusetts recommends the sharing of a debriefing form with workers. For more information see: https://www.umass.edu/research/guidance/mturk-guidance

6. Conclusion and Future Work

As the complexity of AI systems continues to increase, so too will the demand for data enrichment work. It is important that workers at the heart of this growth are respected, supported, and fairly compensated for their contributions. Though there are a number of stakeholders that play a key role in shaping the working conditions of individuals in the data enrichment sector, this paper focuses on recommendations for the sector's clients given their involvement in everyday decisions which directly or indirectly impact workers during the data enrichment process. We hope that equipping clients with an understanding of how their choices impact workers will empower them to make decisions that prioritize worker well-being.

Dedicating attention to worker well-being is all the more important due to the complexity of data supply chains and the lack of standardization in data enrichment practices across the industry. While we acknowledge that there is more work to be done to transform industry practice, this white paper highlights key junctures during the data enrichment process where clients should incorporate worker-oriented thinking into their decision-making process. Specifically, we have examined how clients can incorporate impact on worker well-being into their decision-making process around data enrichment provider selection, running a pilot, task design and writing instructions, task assignment, pricing, communication, quality assurance, and closure and offboarding. We highlight existing research and best practices that clients can incorporate into their decisions.

The data enrichment process has always been an essential part of AI development. Recognizing that AI advances are contingent on data enrichment labor and taking steps to invest in supporting this labor force are similarly essential to the future of this industry. As AI becomes more complex, data enrichment needs and the demands being placed on workers are also growing in complexity. This complexity also creates a need for more workers with specialized knowledge to complete data enrichment work. For the AI industry to grow sustainably, creating the infrastructure to transform data enrichment work into decent jobs is imperative.

Future research and work are needed to address a number of questions:

1. **Systems of Recognition:** Data enrichment work remains largely hidden and done in informal work arrangements. How can workers be recognized for their contributions to the products that rely on data enrichment work? What circumstances are leading to this labor being underrecognized and undervalued today?

2. **Measuring and Evaluating Working Conditions:** How can we work towards a reliable system of evaluation to assess and verify working conditions in the data enrichment sector? What metrics and targets should be adopted around responsible data enrichment sourcing?

3. **Models for Payment and Ensuring Fair Wages:** Is there a way to create a standardized approach to determine a fair price for data enrichment work? How can fair wages be ensured for workers supplying their labor on crowdsourcing platforms?

4. **Transparency:** Given the complex and opaque nature of the data enrichment ecosystem, how can we create greater transparency around data supply chains and the practices undertaken in the industry to source and enrich data?

5. **Standardizing Instructions:** Considering the importance of and difficulty in creating high-quality instructions for data enrichment work, how can we drive towards standard practices that will result in clearer instructions? Are there ways to standardize approaches based on the data enrichment technique being used? For example, are there best practices that can be standardized and used across instructions for image annotation or text sentiment analysis?

6. **Portable Benefits System:** Are existing proposals for portable benefits attainable? Can a portable benefits system function internationally? How can we ensure all data enrichment workers have access to basic benefits like healthcare and paid sick leave?

7. **Evaluating Data Enrichment Work:** On crowdsourcing platforms, are there objective mechanisms that can be developed for evaluating data enrichment work beyond rating systems?

8. **Developing a Deeper Understanding the Data Enrichment Ecosystem:** What forces are currently shaping the data labor market? What interventions are needed to produce better outcomes for workers?

While these questions may be specific to data enrichment work and labor in the context of AI, this work has broader implications for the way labor is organized in society. Much of the precarity that characterizes data enrichment jobs can be attributed to how this labor is algorithmically managed and broken into task-sized chunks, making this critical work appear less like our traditional conceptualization of a "job."[58] As researchers have pointed out, many other jobs are at risk of being fragmented in the same way and might be converted into task-based work in the near future. How task-based work is classified and recognized in society has implications for how labor and "knowledge" is valued within the context of the expanding "knowledge economy." While some data enrichment tasks may seem simple, they require sustained concentration, and often nuanced, domain-specific knowledge and experience. As AI gets more advanced, more people's expertise will be needed to support additional use cases. Recognizing the importance of data enrichment workers and building infrastructure to support them and improve their working conditions is critical to the future of the AI industry.

58 Gray, M.L and Suri. S. 2019. Ghost Work: How to Stop Silicon Valley From Building a New Global Underclass. Houghton Mifflin Harcourt. Google-Books-ID: 8AmXDwAAQBAJ

Annex 1: Existing Tools and Resources for Clients

Crowdsourcing Platform Comparison and Related Resources

Existing tools that can be used by clients to learn more about different practices on crowdsourcing platforms and review research comparing crowdsourcing platforms include:

- **Fair Crowd Work:** Fair Crowd Work provides reviews of crowdsourcing platforms based on the criteria of pay, communication, evaluation, tasks, technology, ability to refuse payment, terms of service, reviews from workers, and reviews from clients.

- **Beyond Mechanical Turk: An Analysis of Paid Crowd Work Platforms:** Researchers at the University of Texas at Austin undertook a cross-platform analysis to see how platforms compare across a number of attributes, including workforce composition, demographics and worker identities represented, mechanisms for tracking qualifications and reputation, management structures, incentive mechanisms, support to ensure quality assurance and control, accessibility of the tool and types of services offered, support for specialized and complex tasks, and promotion of ethics and sustainability.

- **The Online Labour Index:** Developed by the iLabour Project at the Oxford Internet Institute, this index quantifies key measures describing the online gig economy. It tracks labor markets moderated over the internet across countries, primarily through online platforms.

Calculating a Living Wage

Calculating wages for data enrichment workers is complicated due to the international nature of this labor market and due to this work typically being done on a per-task basis. Though we recognize these challenges and acknowledge more work needs to be done to create accessible standards, below are existing tools and resources that can be used to determine a living wage and/or minimum wage:

- **MIT Living Wage Calculator:** Provides living wages in locations across the United States.

- **Anker Methodology:** The Anker methodology calculates a living wage by estimating the cost of a decent lifestyle and taking into consideration housing, healthcare, education, groceries, and transportation as well as deductions, benefits etc.

- **Living Wage Foundation:** Provides accreditation to UK employers who commit to pay a living wage to direct employees and contractors and meet the necessary requirements.

- **Living Wage:** This is an open source tool by OpenUp that will tell a user if they are paying a living wage to domestic workers in South Africa.

- **WageIndicator:** The foundation provides resources and information about living wages for more than 110 countries.

- **Global Living Wage Coalition:** This coalition provides information about living wages in 27 countries across the globe using the Anker Methodology. The coalition defines a living wage as: "The remuneration received for a standard workweek by a worker in a particular place sufficient to afford a decent standard of living for the worker and her or his family. Elements of a decent standard of living include food, water, housing, education, healthcare, transportation, clothing and other essential needs including provision for unexpected events."

- **Fair Wage Guide:** Developed by Good World Solutions, this tool calculates wages and compares them to local and international standards. As a note, the tool only calculates minimum wage and international poverty lines and does not calculate a living wage.

- **Fair Work for Amazon Mechanical Turk:** A tool developed by Stanford researchers that can be used by clients on Amazon Mechanical Turk to "ensure that workers are paid at least a minimum wage."

- **Crowd-Workers:** A browser extension developed by the University of Pennsylvania that enables workers to sort HITs based on an hourly rate.

Task Design and Writing Instructions

Below are existing tools and research that can guide clients in designing tasks and writing instructions:

- **Google Cloud:** Provides guidance on designing and developing instructions for human labelers.

- **Sprout:** An open source tool developed by researchers at the University of Washington and the Indian Institute of Technology that helps clients improve task design on crowdsourcing platforms by collecting feedback from workers, synthesizing this feedback for clients, and providing suggestions to clients to improve task design.

- **TurKit:** A toolkit designed by researchers at MIT "for deploying iterative tasks on mechanical Turk."

- **CrowdWeaver:** Developed by researchers at Carnegie Mellon University, CrowWeaver provides graphical tools to help manage and track worker progress.

- **Structured Labeling:** Researchers at Oregon State University and Microsoft Research have proposed structured labeling solutions to facilitate consistent labeling.

- **Revolt:** Developed by researchers at Carnegie Mellon University and Microsoft Research, Revolt seeks to leverage disagreements to achieve higher label accuracy and create reusable structures with a more nuanced range of labels.

- **Turkomatic:** Developed by researchers at the University of California, Berkeley and Stanford University, Turkomatic seeks to create a collaborative process for workflow design by leveraging input from crowd workers to help clients design and carry out complex tasks.

- **Fantasktic:** Developed by researchers at the University of Berkeley, Fantasktic seeks to improve task design by providing an interface with guidelines and recommendations that can be used by clients, a preview interface that allows clients to see the task from the perspective of the worker or contributor, and automatically generated task tutorials.

- **WingIt:** Developed by researchers at Purdue University, WingIt proposes a system that enables workers to resolve ambiguities in task instructions by enabling workers to ask questions, propose edits to tasks, and discuss ambiguities with other workers. The work calls out three main types of ambiguity in instructions relating to input, process, and output.

Quality Assurance

Existing tools and research that can guide clients in establishing quality assurance practices on crowdsourcing platforms are outlined below:

- **Quality Management on Amazon Mechanical Turk:** Researchers from New York University developed an algorithm that generates an evaluation of quality that takes into account worker bias and error rate for a given worker.

- **Quality Control in Crowdsourcing:** This research provides a comprehensive taxonomy and overview of existing quality control aspects and techniques, a review of quality assurance mechanisms on fourteen different platforms, and proposes a model for crowdsourcing platforms built around people.

- **How Many Workers to Ask?: Adaptive Exploration for Collecting High Quality Labels:** Research that explores the question of how many workers are needed to complete a task to ensure statistically significant results through the development of an algorithm that draws upon the quality score of a worker and the difficulty of a hit.

- **Quality Control in Crowdsourcing Systems: Issues and Directions:** Researchers have provided a taxonomy of quality and quality assurance techniques where quality is characterized by task design and worker profiles.

- **Quality Management in Crowdsourcing using Gold Judges Behavior:** Research that explores the effectiveness of embedding known answers as a method to ensure quality. This research ultimately concludes that embedding gold-standard known "answers" is a useful technique to improve quality.

Annex 2: Considerations for Service Provider Selection

Below are worker-oriented considerations that clients should weigh when selecting a service provider for data enrichment work.

1. Commitment to Labor Standards, Worker-Oriented Policies, Ethical Sourcing, and Sustainability

Criteria: Clients should consider and analyze what commitments a prospective service provider has made to adhere to labor standards and ethical sourcing. While some service providers may have certifications demonstrating they have met the standards of an independent agency, others may articulate commitments on their own. It is important to consider both the commitments they have made and how they can be held accountable for those commitments. If a service provider does not explicitly mention any worker oriented policies or standards, explicitly asking them can help push them to provide greater transparency over their practices and provide a powerful signal that this is an important consideration for clients.

In evaluating service providers' commitments, clients can refer to the recommendations made in this paper to see how potential providers' practices compare and consult a number of applicable international instruments and standards. A few standards to refer to are the UN Guiding Principles on Business and Human Rights, key labor rights and principles defined by the International Labor Organization, and the Global Impact Sourcing Coalition's "Impact Sourcing Standard." When it comes to assessing crowdsourcing platforms, there are additional factors that need to be evaluated for their impact on workers, including: the code of conduct, the privacy policy, security policy, terms of service (particularly in terms of how they handle workers' accounts being suspended or terminated), and policy for resolving disputes (such as handling disputes over rejected work, nonpayments, and ratings).

For a full list of relevant tools, refer to Annex 2: International Guidance, Standards, Certifications, and Codes of Conduct for Supply Chains, and Principles and Best Practices for Crowdsourcing Platforms.

Explanation: The policies that govern service providers and crowdsourcing platforms can significantly impact outcomes for workers by shaping workers' abilities to own/access the information that is provided and generated by them,[59] understand and control how such information is used by the service,[60] navigate systems of management and recognition including the ability to contest an action taken against them, and provide feedback on their experiences.

2. Clarity on Benefits

Criteria: It is important to assess the benefits and support programs available to workers engaged with a particular service, such as shared benefits like micro-insurance or portable benefits.

59 O'Conner, Sarah. Let Gig Workers Control Their Data Too. Financial Times. April 3rd 2018. Accessed September 5th 2020. https://www.ft.com/content/a72f7e56-3724-11e8-8b98-2f31af407cc8

60 Sergison, Danica. Privacy risks for customers and workers in the gig economy. Privacy News Online. September 2nd 2018. Accessed September 5th 2020. https://www.privateinternetaccess.com/blog/privacy-risks-for-customers-and-workers-in-the-gig-economy/

Explanation: Individuals working on crowdsourcing platforms are often categorized as independent contractors and work on short-term contracts. This is also the case for some workers working with managed services. Existing labor laws do not always adequately cover independent contractors which can result in job insecurity, lack of benefits, and lack of access to organizing opportunities and labor unions.[61]

Micro-insurance[62] and portable benefits[63] have been explored as potential solutions to ensure workers on crowdsourced services receive the benefits they need. However, it is important to call out that this is an area that needs further investigation, research, and progress. Furthermore, solutions should not be limited to portable benefits. Addressing inconsistent pay, low wages, transaction costs, and lack of benefits are all challenges that need to be addressed in order to make these jobs sustainable for workers.[64] Regulators and policymakers have started exploring challenges around employment statuses for crowdworkers. An outline of emerging law and policy that is applicable to crowdsourcing platforms can be found in Annex 2: National Legislation and Policy.

3. Commitment to Transparent Pricing and Base Wage

Criteria: Reviewing the service providers' pricing methodology is an essential part of assessing their approach to worker well-being. If the pricing and wages for workers are unclear, explicitly asking for clarity over how service providers pay workers can push them to provide more transparency overall. In addition to pricing and wages, obtaining more information from service providers about the workforce itself, including geographic locations, are crucial in order to evaluate if the wages are acceptable. Other relevant practices to ask for clarity around include methods and forms of payment, bonuses, promotions, access to work, regularity of work provided to workers, handling of equipment costs, if wages grow over time, and approach to wage negotiations.[65] Such information can be indicated within the engagement contract or may be established organization-wide through accreditation from bodies like the Living Wage Foundation.[66]

61 Towards a Fairer Gig Economy. Meatspace Press 2017. Accessed September 20th 2020. https://ora.ox.ac.uk/objects/uuid:de091436-0482-4818-8c87-ff89707f8339/download_file?file_format=pdf&safe_filename=Towards_A_Fairer_Gig_Economy.pdf&type_of_work=Book and Robertson, Pete. How the Gig Economy Creates Job Insecurity. BBC. September 18th 2017. Accessed September 5th 2020. https://www.bbc.com/worklife/article/20170918-how-the-gig-economy-creates-job-insecurity, and Kapoor, Astha, Natarajan, Sarayu. Productivity Vs. Well-Being: The Promise of Tech Mediated Work and Its Implications on Society. Observer Research Foundation. October 5th 2019. Accessed September 5th 2020. https://www.orfonline.org/expert-speak/productivity-vs-well-being-the-promise-of-tech-mediated-work-and-its-implications-on-society-56962/

62 For example see: Micro insurance. Accessed September 5th 2020. https://www.microinsurance.com/micro-insurance-services#products, and Next Billion. Accessed September 5th 2020. https://nextbillion.net/microinsurance-for-gig-economy/, https://home.kpmg/xx/en/home/insights/2019/05/insuring-the-gig-economy.html and Freelancers Union. Accessed September 5th 2020. https://www.freelancersunion.org/insurance/health/

63 Defined by the Aspen Institute as an arrangement where "benefits are connected to an individual, rather than a particular employer, and so they can be taken from job to job without interruption in coverage or loss of funding." The Aspen Institute. Non-Traditional Work. Accessed September 5th 2020. https://www.aspeninstitute.org/programs/future-of-work/nontraditional-work/#:~:text=Portable%20benefits%20are%20connected%20to,be%20funded%20from%20multiple%20sources and Hill, Steven. New Economy, New Social Contract. New America. August 2015. Accessed September 5th 2020. https://static.newamerica.org/attachments/4395-new-economy-new-social-contract/New%20Economy,%20Social%20Contract_UpdatedFinal.34c973248e6946d0af17116fbd6bb79e.pdf

64 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons from a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

65 Vakharia, Donna. Lease, Mathew. Beyond Mechanical Turk: An Analysis of Paid Crowd Work Platforms. University of Texas-iConference. 2015. Accessed September 5th 2020. https://www.ischool.utexas.edu/~ml/papers/donna-iconf15.pdf

66 The Living Wage Foundation. Accessed September 5th 2020. https://www.livingwage.org.uk/

Explanation: While data enrichment work can be a source of additional income and economic opportunity for some individuals, it is a primary source of income for others. Many pricing and payment models adopted by platforms have resulted in low prices.[67] Increasing transparency over pricing is an essential step towards pushing for better wages for data enrichment professions. Clients are in a unique opportunity to help increase transparency in the industry by explicitly asking about how wages are set when working with a service provider. Some suggestions for improving pricing practices have included having companies publish data on rates and wages to enable comparative analysis, classifying freelancers as employees, instituting a minimum task rate based on a minimum wage, and developing a wage range that is based on the experience of the independent contractor.[68]

Additional information about how clients can approach pricing is outlined in the section Defining Payment Terms and Pricing.

4. Opportunities for Recognition and Reputation Visibility

Criteria: Clients should also consider what opportunities are in place for personal and professional development including recognition and career mobility. A few ways to measure service providers' actions in this area include whether they have a portablue reputation system or comparable solution, how they measure qualifications, their process for evaluating and rewarding workers, their approach to promotions, and whether they provide training or educational opportunities for workers to obtain new skills.

Explanation: While data enrichment work is getting increasingly sophisticated and requires more specialized skills, many have pointed out how this work is often undefined, unrecognized, and underappreciated.[69] This can partly be attributed to the way AI is marketed as a technological advance that can be more efficient than humans. Acknowledging the high labor costs necessary to train AI models runs counter to this narrative.[70] However, a lack of recognition and meaningful career advancement opportunities is problematic for workers.

Workers on crowdsourcing platforms are often dependent on clients to provide ratings and statistics about the type of tasks they have completed. Yet research has noted that ratings on crowdsourcing platforms can be inaccurate and undependable.[71] Some crowdsourcing platforms use "badge" systems to distinguish workers' skills and some have processes in place to promote workers to different levels (leadership, expert, trainer, etc.).[72] Crowdsourcing platforms can also claim ownership over information on the platform including reviews, ratings, and feedback.[73]

67 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons from a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf and Metz, Cade. A.I. Is Learning from Humans. Many Humans. New York Times. August 16th 2019. Accessed September 5th 2020. https://www.nytimes.com/2019/08/16/technology/ai-humans.html

68 Caitlin Lustig, Sean Rintel, Liane Scult, and Siddharth Suri. 2020. Stuck in the Middle With You: The Transaction Costs of Corporate Employees Hiring Freelancers. Proc. ACM Hum.-Comput. Interact. 4, CSCW1, Article 37 (May 2020), 28 pages. https://doi.org/10.1145/3392842

69 Whittaker, Meredith. Crawford, Kate. AI Now Report 2018. AI Now Institute. December 2018. Accessed September 5th 2020. https://ainowinstitute.org/AI_Now_2018_Report.pdf

70 Gray, M.L and Suri. S. 2019. Ghost Work: How to Stop Silicon Valley From Building a New Global Underclass. Houghton Mifflin Harcourt. Google-Books-ID: 8AmXDwAAQBAJ

71 Whiting, Mark. Gamage, Dilrukshi. Crowd Guilds: Worker- led Reputation and Feedback on Crowdsourcing Platforms. https://arxiv.org/pdf/1611.01572.pdf

72 Vakharia, Donna. Lease, Mathew. Beyond Mechanical Turk: An Analysis of Paid Crowd Work Platforms. University of Texas-iConference. 2015. Accessed September 5th 2020. https://www.ischool.utexas.edu/~ml/papers/donna-iconf15.pdf

73 For example, the Terms of Service for Freelancer state: "You acknowledge that you transfer copyright of any feedback, reputation or reviews you leave consisting of comments and any rating(s) (e.g. quality, communication etc.) together with any composite rating by us. You acknowledge that such feedback, reputation and reviews belong solely to us, notwithstanding that we permit you to use it on our Website while you remain a User. You must not use, or deal with, such feedback, reputation and reviews in any way inconsistent with our policies as posted on the Website from time to time without our prior written permission." For more information see: Freelancer User Agreement. Accessed September 5th 2020. https://www.freelancer.com/about/terms#

This restricts workers ability to move their work and profiles from one service to another and "locks" them[74] into a particular platform because they would have to start from scratch if they started working on another platform.[75] This puts workers at a disadvantage in terms of their negotiating power. It also puts them in a risky situation in the event their account is closed and they lose the reputation they have developed on a particular platform.[76] In response to this challenge, research has recommended that workers have the ability to export human and machine readable work histories in order to empower workers to continue work relationships, independent of any platform.[77] Recommendations for strong "portable reputation" systems include being worker-controlled, transparent, reparable with improved work, able to incorporate input and reviews from multiple companies, resistant to bias and prejudice, fair in how they distribute rewards, and equipped with a grievance process.[78] Some features of portable reputation systems that are being researched include incorporating personal references, being publicly hosted, providing profile verification, having decentralised open data standards, and having a centralised data holder.[79]

5. Provision of Work Space and Communication

Criteria: When engaging with a service, it can be useful for a client to consider what physical and/or virtual workspaces are available to workers and if the workers work out of an ISO certified facility.[80] Additional considerations include the type of environment being provided for workers at physical facilities such as amount of space per person, lighting, equipment, air-quality, etc. If engaging with a crowdsourcing platform, it can be useful to consider what policies, systems, or forums are in place to allow workers to communicate with other workers, clients, and platform administrators.

Explanation: Research has noted the impact that remote work and disaggregated tasks can have on workers.[81] For crowdsourcing platforms in particular, researchers have pointed out that improvements can be made in facilitating communication between workers, clients, and administrators.[82] As mentioned in the paper, better communication can benefit workers and clients by making sure there are efficient ways to resolve uncertainties, which can in turn impact the project timeline. While some crowdsourcing platforms provide methods for workers to communicate with each other, this is rare enough that a number of organic communities and networks outside of platforms have formed as spaces for workers to share experiences and help each other navigate this work. For example, forums like Turkopticon have emerged to provide workers with a means of evaluating and navigating clients.[83] Researchers have underscored the need for these types of networks and spaces for workers to build community, particularly when unions are not present.[84]

74 https://magazine.seats2meet.com/research-on-platform-based-reputation-scores-contributes-to-an-inclusive-labor-market/
75 Sipp, Kati. Ratings in the Gig Economy Are a Mess. Here's How to Fix Them. Wired. December 27th 2017. Accessed September 5th 2020. https://www.wired.com/story/how-to-fix-ratings-in-the-gig-economy/
76 Robinson, Carrie. Exploring Portable Ratings for Gig Workers. Medium. February 2nd 2020. Accessed September 5th 2020. https://medium.com/doteveryone/exploring-portable-ratings-for-gig-workers-5632fd9b262e
77 Berg, Janine, Furrer, Marianne. Digital Labour Platforms and the Future of Work. International Labour Organization. 2018. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_645337.pdf
78 Sipp, Kati. Ratings in the Gig Economy Are a Mess. Here's How to Fix Them. Wired. December 27th 2017. Accessed September 5th 2020. https://www.wired.com/story/how-to-fix-ratings-in-the-gig-economy/
79 Robinson, Carrie. Exploring Portable Ratings for Gig Workers. Medium. February 2nd 2020. Accessed September 5th 2020. https://medium.com/doteveryone/exploring-portable-ratings-for-gig-workers-5632fd9b262e
80 For example, see: https://www.iso.org/standard/68021.html
81 Hui, Julie, Cranshaw, Justin, Kotturi, Yasmine, Kulkarni, Chinmay. The Future of Work(places): Creating a Sense of Place for On-Demand Work. CSCW'19: Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing. November 2019. Accessed September 5th 2020. https://doi.org/10.1145/3311957.3359432
82 Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons from a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf
83 Turkopticon is a community and tool to enable workers to rate requesters on factors such as communicativity, generosity, fairness, and promptness. For more information see: https://turkopticon.ucsd.edu/
84 Wood, Alex, Lehdonvirta, Vili, Graham, Mark. Workers of the Internet Unite? Online Freelancer Organisation Among Remote Gig Economy Workers in Six Asian and African Countries. New Technology, Work and Employment. Volume, Issue 2. July 10th 2018. Accessed September 5th 2020. https://doi.org/10.1111/ntwe.12112

6. Systems for Diversity

Criteria: Clients should also assess if there are processes and mechanisms in place to support workforce diversity in terms of skill set, background, and geography. Particularly when engaging with a crowdsourcing platform, it is useful to consider what mechanisms are available to incorporate diversity or a targeted background. For example, analyze which filters are available to select a workforce for a given project. This also requires having an understanding of what diversity means, the type of diversity needed for a particular project, and how diversity is measured.

Explanation: Given the nature of data enrichment work, where individual perspectives and experiences can lead to various workers interpreting tasks differently, it is important to take diversity or composition of the workforce into consideration.[85] Research has spotlighted the important role played by data quality, diversity, and accuracy in shaping machine learning models.[86] Depending on the type of data that is being curated and the technique being used, there is also potential for bias to be introduced into enriched datasets. For example, research has found that tasks like sentiment analysis or content moderation involve more subjective determinations and are subject to human bias.[87]

7. Content Policies

Criteria: For projects that involve working with data or content that is either violent or age-sensitive, clients should consider what policies and support are in place to protect workers.

Explanation: Some tasks may involve being exposed to graphic or violent content that needs to be viewed, annotated, cleaned, or otherwise handled for extended periods of time. Research has documented the negative impact that extended exposure to such content can have on workers.[88] To address this, researchers have stressed the importance of providing support for workers and adopting policies that take the risks of this exposure into account.[89]

85 Barbosa, Nata, Chen, Monchu. Rehumanized Crowdsourcing: A Labeling Framework Addressing Bias and Ethics in Machine Learning. In CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK. ACM, New York, NY, USA. https://www.natabarbosa.com/chi_rehumanized_crowdsourcing.pdf

86 Redman, Thomas. If Your Data Is Bad, Your Machine Learning Tools Are Useless. Harvard Business Review. April 2nd 2018. Accessed September 5th 2020. https://hbr.org/2018/04/if-your-data-is-bad-your-machine-learning-tools-are-useless

87 Barbosa, Nata, Chen, Monchu. Rehumanized Crowdsourcing: A Labeling Framework Addressing Bias and Ethics in Machine Learning. In CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK. ACM, New York, NY, USA. https://www.natabarbosa.com/chi_rehumanized_crowdsourcing.pdf

88 Roberts, Sarah T. Content Moderation in the Shadows of Social Media. Yale University Press. June 5th 2019.

89 89Berg, Janine, Furrer, Marianne, Harmon Ellie, Rani, Uma, Silberman M. Six. Income Security in the On-Demand Economy: Findings and Policy Lessons from a Survey of Crowdworkers. International Labour Office. 2016. Accessed September 5th 2020. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_479693.pdf

Annex 3: Existing Guidance for Human Rights, Workers Rights, Supply Chain, and Platforms

This section outlines key international guidelines and tools related to workers rights, human rights, and ethical sourcing. It also covers emerging legislation around the "platform economy" and best practices for crowdsourcing platforms. The intention of this section is to provide clients with a brief overview of each resource as a starting point to undertake a deeper investigation into emerging standards relevant to ethical data enrichment.

International Guidance

There are a number of international standards for ensuring human rights and worker rights. These include:

ILO Declaration on Fundamental Principles and Rights at Work: As defined by the International Labor Organization, fundamental principles and rights at work include: freedom of association and the right to collective bargaining, elimination of forced or compulsory labor, abolition of child labor, and elimination of discrimination. The ILO has also developed International Labor Standards around basic human rights, occupational safety and health, wages, working time, employment policy and promotion, vocational guidance and training, skills development, specific categories of workers, labor administration and inspection, maternity protection and social security, indigenous and tribal people, and migrant workers.

United Nations Guiding Principles on Business and Human Rights: The UN Guiding Principles present a framework based on states' duties to protect human rights, the corporate responsibility to respect human rights, and states' obligation to provide access to remedy in cases of human rights abuses. The principles outlined here are meant to apply to organizations across different industries, sizes, regions, operational contexts, and ownership structures. The principles refer to the International Bill of Human Rights and the rights set out by the ILO in order to provide guidance to businesses on how to embed human rights due diligence into their processes. In doing so, the principles place a positive obligation on businesses to avoid, prevent, mitigate, and address adverse impacts to human rights. Key recommendations for companies include adopting policy commitments articulating a responsibility to respect human rights, a due diligence process to address their impacts on human rights, and mechanisms to provide remedy for any adverse impacts to human rights.

The United Nations Global Compact: The UN Global Compact articulates 10 principles to guide organizations in responsible business practice in the areas of human rights, labor, environment, and anti-corruption. These principles are grounded in the UDHR, the ILO principles, the Rio Declaration on Environment and Development, and the United Nations Convention Against Corruption.

United Nations Sustainable Development Goals: These outline key goals related to poverty, inequality, climate change and more. Sustainable Development Goal 1 pertains to ending poverty in all its forms everywhere and Goal 8 pertains to decent work and economic growth.

ILO Tripartite Declaration of Principles for Multinational Enterprises and Social Policy: The declaration provides guidance to national and multinational companies on how to develop and implement inclusive, responsible, and sustainable workplace practices which create decent work for all, and enable economic and social progress. The principles focus on employment, training, conditions of work and life, and industrial relations. More specifically, the principles outline the importance of promoting employment opportunities, providing social security, eliminating forced or compulsory labor, abolishing child labor, promoting equal opportunity and treatment, providing secure employment, providing relevant training opportunities, ensuring fair wages and benefits, providing a safe and healthy environment, protecting the freedom to associate and organize, ensuring workers can collectively bargain, and guaranteeing workers have access to remedy, and facilitating processes to settle industrial disputes.

Universal Declaration of Human Rights (UDHR): The UDHR articulates human rights including right to equality, freedom from discrimination, right to life and liberty, right to personal security, freedom from slavery, freedom from torture and degrading treatment, right to recognition as a person before the law, right to equality, right to remedy by a competent tribunal, freedom from arbitrary arrest and exile, right to a fair public hearing, right to be considered innocent until proven guilty, freedom from interference with privacy, family, home, and correspondence, right to free movement in and out of the country, right to asylum in other countries from persecution, right to a nationality and freedom to change it, right to marriage and family, right to own property, freedom of belief and religion, freedom of opinion and information, right of peaceful assembly and association, right to participate in government and free elections, right to social security, right to desirable work and to join trade unions, right to rest and leisure, right to adequate living standard, right to education, and right to participate in cultural life of community.

International Covenant on Civil and Political Rights (ICCPR): Adopted in 1966, the ICCPR articulates a commitment for members to respect the civil and political rights of individuals including the right to life, freedom of religion, freedom of speech, freedom of assembly, electoral rights, and right to due process.

Standards, Certifications, and Codes of Conduct for Supply Chains

Ethical supply chain practices have traditionally been articulated and audited against a number of different standards and certifications. These have been developed to address concerns around professionalism, working conditions, ethical business practices, transparency and accountability, due diligence, and legal compliance. Companies have also committed to individual codes of conduct and ethical sourcing frameworks. In some sectors, such as textiles and manufacturing, such practices and standards have evolved to be comprehensive. While these are still developing for data enrichment, there are some examples of standards and frameworks that are potentially relevant to companies involved in data enrichment services:

- **Impact Sourcing Standard:** This model outlines minimum requirements necessary for businesses to ensure employees earn an equitable or living wage while meeting business objectives. The Global Impact Sourcing Coalition is a network of individuals and organizations working to build inclusive global supply chains through the adoption of Impact Sourcing. The Coalition offers a standard and a self-assessment tool that is built around five pillars: commitment to impact sourcing, recruiting and hiring, remuneration and benefits, training and career development, and management systems for impact sourcing.

- **Social Accountability International SA800:** This is a social certification program by Social Accountability International that is based on the UDHR and ILO conventions. This standards covers areas such as child labor, forced labor, health and safety, freedom of association and collective bargaining rights, discrimination, discplinary practices, working hours, remuneration, and management system.

- **Ethical Labor Sourcing Standard, BES, 6002:** This framework for ethical labor sourcing governance standard was developed by the BRE group. The framework covers company structure, management policies, management systems, assurance auditing, HR, immigration, supply chain management, bribery, L&D, forums, and reporting. While the framework can be used by a company to assess their own practices, BRE also provides an Ethical Labor Sourcing verification based on this framework.

Principles and Best Practices for Crowdsourcing Platforms

There are emerging standards and codes of conduct that speak directly to crowdsourcing platform work. Examples of principles and best practices that clients can use to understand best practices when engaging with a crowdsourcing platform include:

- **Crowdsourcing Code of Conduct:** Developed in 2017, the Code of Conduct outlines ground rules towards enabling fair and prosperous cooperation between crowdsourcing companies and crowdworkers that can be adopted by platforms and regulators.

- **Manifesto for the Gig Economy:** Developed by Antonio Aloisi, Valerio De Stefano, and Six Silberman, this manifesto articulates a set of goals for platforms, policymakers, and unions to ensure a "healthy digital transition."

- **Frankfurt Declaration on Platform Based Work:** Developed in 2016, the Declaration articulates seven commitments to govern digital labor platforms which can be adopted by platforms and regulators. These commitments address fair working conditions and worker participation.

- **Fairwork Foundation Principles for Online Work:** The Fairwork Foundation aims to enable voluntary scoring of platforms, facilitate ethical choices by stakeholders in the ecosystem, and improve working conditions for those partaking in the digital platform economy. The framework allows for the evaluation of platforms based on principles of pay, conditions, contracts, management, and representation. It also includes specific principles in these areas that apply to online work and gig work.

- **Model Rules on Online Platforms:** Developed by the European Law Institute, Model Rules on Online Platforms evaluates the relationship between platform operators and users, addresses questions of platform liability, sets minimum requirements for fairness and transparency, considers designs of reputation systems, and explores structures for the right to portability.

Comparative Table of Principles and Best Practice for Crowdsourcing Platforms				
Principle/Code	**Categorisation**	**Rights/Benefits**	**Wages and Payment**	**Framework for work**
Crowdsourcing Code of Conduct	N/A	N/A	• Commitment to provide fair payment • Advise requesters on how to calculate fair wages by taking into consideration factors like task complexity, qualifications, local wage standards, and timeframe for tasks	• Ensure work offered on a platform is legal and indicate when content might be age specific • Clarify applicable regulations • Offer motivating and good work • Enable respectful interactions • Provide clear tasks and reasonable timeframes • Enable freedom and flexibility of workers, including removing penalties for workers who refuse work
Manifesto for the Gig Economy	• Recognize platform "regulars" as employees • Policymakers to regulate gig economy like a form of casual employment	• Support forms of unionizing and organizing • Ensure high working standards and conditions including protection against discrimination, access to collective bargaining, health and safety measures, a living wage, training opportunities, and ownership over one's own work	• Ensure a living wage • Ensure transparency in payment rules • Clarify minimum levels of payment	• Provide code of conduct that clarifies payment, rating criteria, and transparency of internal processes • Provide a dispute resolutions mechanism • Provide good working standards to all platform contributors • Provide a portable rating system
Frankfurt Declaration on Platform Based Work	• Clarify employment status of platform based workers	• Ensure all nonself-employed workers have the right to organize • Ensure access to social protection	• Ensure at least a minimum wage in their jurisdiction	• Develop dispute resolution mechanisms • Increase transparency in platform work • Ensure legal compliance with national laws and international instruments
Model Rules on Online Platforms		• Platforms have a duty to protect users • Address misleading information given by users • Provide reporting mechanisms and redress mechanisms		• Ensure that contract terms are clear, machine readable, and available to platform users at all stages of the engagement–users should be notified of any changes • Information about the parameters determining ranking should be provided to users • Users should be informed if the result of a search query has been influenced by financial or corporate ties between a platform and the supplier • Users should be informed about how and what information is used in reputation systems • Platforms must ensure reviews meet the standards of professional diligence • Reviews should be portable • Facilitate communication between customers and suppliers as needed

Fairwork Foundation Principles for Online Work		• Platforms should have policies in place to protect workers and promote the health and safety of workers • Platforms should provide a process through which workers can express their thoughts and organise	• Workers should earn a decent income relative to their home jurisdiction—this should take into consideration work-related costs and active hours worked • Workers should be paid on time • Workers should be paid for all work completed	• Platform terms of service should be transparent and accessible to workers • The party contracting with the worker should be subject to local laws and identified in the contract • Changes to terms of services should be clearly communicated to workers • Workers should be permitted to seek redress for grievances • Workers should have access to documented due process and mechanisms for appeal • Contracts should be consistent with terms of workers' engagement on the platform • Any use of algorithms should be transparent and result in equitable outcomes • A policy should ensure equity in the management of workers on the platform`

National Legislation and Policy

Policymakers, governments, and courts around the world are beginning to take steps to provide regulatory clarity around protections for individuals working as freelancers and on temporary contracts, particularly those working through digital labor platforms. This includes clarity in aspects such as the categorization of workers, wage requirements, eligibility for benefits and entitlements, and acceptable conditions for work. While some of these efforts have been met with appreciation, others have been met with criticism and concern of unintended consequences such as limiting the ability of individuals to work as freelancers if they choose and increased difficulty in finding a job if organizations extend benefits to a larger group of workers.[90] This demonstrates that best practices are still emerging. A nuanced approach is needed to craft regulation governing the digital economy in order to improve working conditions for workers, while minimizing unintended consequences. At the moment, there appear to me more legislative developments focused on specific types of work in the gig economy, such as through transportation platforms and apps.

The table below summarizes some of the developments and regulatory trends that are emerging globally. Please note that the table is not exhaustive:

90 For example, the discourse around AB5 has recognized it as having both positives and negatives. For more information see: https://www.washingtonpost.com/business/2020/01/14/can-california-reign-techs-gig-platforms-primer-bold-state-law-that-will-try/

Comparative Table of Regulatory Developments for the Gig Economy		
Legislation/feature	**Scope/Categorization**	**Rights**
EU Rules for Gig Economy 2020[91]	Workers on "atypical contracts" and working +12hrs p/m	• Entitled to receive information about the essential aspects of a job within a week • Entitled to receive compensation if there is late cancellation of work • Access to free mandatory training • Limit of six month probationary period • Ban on "exclusivity clauses" for workers
California Gig Economy Law AB5[92]	Categorized as an employee unless the worker is: (a) Free from the control and direction of the hiring entity in connection with the performance of the work. (b) performs work that is outside the usual course of the hiring entity's business. (c) Engaged in a similarly but independently established trade, occupation, or business of the same nature.	If categorized as employee, guaranteed minimum wage, workers' compensation if they are injured on the job, unemployment insurance, paid sick leave, and paid family leave.
Indian Code on Social Security 2019[93]	Expands the definition of the unorganized sector to include gig, platform, contract, migrant, and domestic workers.	Social schemes for unorganized workers which can include benefits such as life and disability cover, health and maternity benefits, old age protection, education, housing, PF, employment injury benefit, housing, child care, skilling, funeral assistance, and old age homes.
Protecting the Right to Organize Act 2019[94]		Give workers more power in work related disputes, penalize companies violating labor law, protect against misclassification of freelance workers and ensure that workers have access to collective bargaining rights.

91 In April 2020, as part of the EU's social policy, the European Parliament passed Rules to ensure rights and set a standard for working conditions for individuals working on 'atypical' contracts.European Parliament. Gig Economy: EU law to improve workers rights infographic. Last updated July 11th 2019. Available at: https://www.europarl.europa.eu/news/en/headlines/society/20190404STO35070/gig-economy-eu-law-to-improve-workers-rights-infographic and European Parliament. Briefing. Ensuring more transparent and predictable working conditions. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/628269/EPRS_BRI(2018)628269_EN.pdf

92 Coming into effect on January 1st 2020, AB5 expands the definition of what constitutes an employee. For more information see: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB5 and

93 https://labour.gov.in/sites/default/files/375_2019_LS_Eng.pdf

94 https://www.congress.gov/bill/116th-congress/house-bill/2474/text

Artificial Intelligence in Finance: Putting the Human in the Loop

Zetzsche, DA
Arner, DW
Buckley, RP
Tang, B

University of Hong Kong Faculty of Law Research Paper No. 2020/006

CFTE Centre for Finance, Technology and Entrepreneurship

CFTE ACADEMIC PAPER SERIES

Artificial Intelligence in Finance: *Putting the Human in the Loop*

Dirk A. Zetzsche I Douglas Arner
Ross Buckley I Brian W. Tang

VOLUME 1 2020

CFTE

CFTE curates & selects some of the worlds leading research on the topic of finance and technology. Full versions of our papers are accessible on this link: https://cfte.education/academicpapers/

CFTE is an education platform supported by senior leaders from the largest institutions, startups and universities. It addresses the needs of professionals in finance and technologists to upskill in a rapidly changing industry being transformed by emerging technologies.

Artificial Intelligence in Finance:
Putting the Human in the Loop

Dirk A. Zetzsche[*]

Douglas Arner[**]

Ross Buckley[***]

Brian W. Tang[****]

February 2020

Finance has become one of the most globalized and digitized sectors of the economy. It is also one of the most regulated of sectors, especially since the 2008 Global Financial Crisis. Globalization, digitization and money are propelling AI in finance forward at an ever increasing pace.

This paper develops a regulatory roadmap for understanding and addressing the increasing role of AI in finance, focusing on human responsibility: the idea of "putting the human in the loop" in order in particular to address "black box" issues.

Part I maps the various use-cases of AI in finance, highlighting why AI has developed so rapidly in finance and is set to continue to do so. Part II then highlights the range of the potential issues which may arise as a result of the growth of AI in finance. Part III considers the regulatory challenges of AI in the context of financial services and the tools available to address them, and Part IV highlights the necessity of human involvement.

We find that the use of 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

[*] Professor of Law, ADA Chair in Financial Law (Inclusive Finance), Faculty of Law, Economics and Finance, University of Luxembourg, and Director, Centre for Business and Corporate Law, Heinrich-Heine-University, Düsseldorf, Germany.

[**] Kerry Holdings Professor in Law and Director, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong; Adviory Board Member, Centre for Finance, Technology and Education.

[***] KPMG Law and King & Wood Mallesons Chair of Disruptive Innovation, Scientia Professor, and Member, Centre for Law, Markets and Regulation, UNSW Sydney. Professor Buckley chairs the Digital Finance Advisory Panel of the Australian Securities and Investments Commission (ASIC) however the views expressed herein are strictly his own, not those of ASIC.

[****] Founding Executive Director, LITE Lab@HKU, Faculty of Law, University of Hong Kong, Co-chair of the FinTech Association of Hong Kong's RegTech Committee, Co-Founder, Asia Capital Market Institute (ACMI) and member of the IEEE Global Initiative in Autonomous and Intelligent Systems' Policy Committee.

The authors thank the Hong Kong Research Grants Council Research Impact Fund and the Qatar National Research Fund National Priorities Programme for financial support.

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, we argue for strengthening 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 in our view 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.

Contents

Introduction

The concept of artificial intelligence – AI – is the focus of much global attention today.[1] While AI has a long history of development, technological advances combined with ever-widening digitization have underpinned recent rapid and unprecedented evolution. Central to the "Fourth Industrial Revolution" and the "digitization of everything" is the impact of datafication – manipulation of digitized data through quantitative data analytics, including AI.[2]

From a positive standpoint, AI is expected to contribute to problem solving in and development of most sectors of the economy and society. PwC's optimistic expectations are that AI will boost global GDP by 14% or US$15.7 trillion – by 2030.[3] In the context of finance, Accenture estimates that banks can expect potential savings of between 20% and 25% across IT operations, including infrastructure, maintenance and development costs.[4] The combination of cost savings and enhanced efficiency combined with the potential for entirely new business models and opportunities explains why financial services companies are expected to spend a US$11 billion on AI in 2020, more than any other industry.[5]

At the same time, AI and automation are raising major concerns, ranging from widespread job losses[6] to the possible advent of the "singularity": the point at which the capacities of general AI surpass that of humans in essentially every way. These concerns have triggered an increasing range of analyses of the policy, legal and regulatory implications of AI, from ethical dimensions[7] to legal restrictions.[8] Central to many of these discussions are the role of humans in the evolution of AI: the necessity of involving people in using, monitoring and supervising AI in order to reduce the likelihood of problems arising and their severity. This is the idea of putting a "human in the loop", and it is the challenge at the heart of AI governance discussions in all sectors, all over the world.

---

[1] *See*, for instance, the literature survey by Bonny G. Buchanan, "Artificial intelligence in finance services" (The Alan Turing Institute, April 2019) < https://www.turing.ac.uk/sites/default/files/2019-04/artificial_intelligence_in_finance_-_turing_report_0.pdf>.

[2] *See* UK Finance and Microsoft, "Artificial Intelligence in Financial Services" (27 Jun. 2019) 5 < https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/artificial-intelligence-financial-services≥.

[3] PricewaterhouseCoopers, "Sizing the prize: What's the real value of AI for your business and how can you capitalise?" (2017) 4< https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf>.

[4] AI Accenture, "Redefine Banking with Artificial Intelligence" (2018) 9 > https://www.accenture.com/_acnmedia/pdf-68/accenture-redefine-banking.pdf>.

[5] *See* International Data Corporation (IDC), report May 2019, cited by Amy Zirkle, The Critical Role of Artificial Intelligence in Payments Tech, 27 May 2019, < https://www.fintechnews.org/the-crirital-role-of-artificial-inteliigence-in-payments-tech/>.

[6] *See* Shelly Hagan, More Robots Mean 120 Million Workers Need to be Retrained', 6 Sept 2019, https://www.bloomberg.com/news/articles/2019-09-06/robots-displacing-jobs-means-120-million-workers-need-retraining (citing an IBM survey stating that 120 million jobs will be lost due to AI within the next 3 years).

[7] *See* Dirk Helbing, 'Societal, Economic, Ethical and Legal Challenges of the Digital Revolution: From Big Data to Deep Learning, Artificial Intelligence, and Manipulative Technologies' in Dirk Helbing (eds), *Towards Digital Enlightenment* (Springer, 2018).

[8] *See*, as one of the earlier scholarly articles, Harry Surden, "Machine learning and the law", 89 Wash. L. Rev. 87 (2014).

In the context of AI and AI governance, one area which has until very recently received relatively less attention is the role of AI in finance.[9] This is surprising because finance has become one of the most globalized and digitized sectors – if not the most globalized and digitized sector – of the world's economy. It is also one of the most regulated of sectors, especially since the 2008 Global Financial Crisis. Not surprisingly, AI is already playing an important role in finance, and one that is only likely to grow due to the nature of the financial industry and the ongoing process of global digital financial transformation. As a result, issues around AI and AI governance are growing in significance in finance. Finance however as a result of regulatory developments since the Global Financial Crisis, also provides an important opportunity to address the human in the loop challenge.

This paper develops a regulatory framework for understanding and addressing the increasing role of AI in finance, focusing on human responsibility within the context of putting the "human-in-the-loop" as a core approach in addressing "black box" problems with AI.

Part I maps the various use-cases of AI in finance, highlighting why AI is developing so rapidly in finance. Part II highlights the range of potential issues which may arise as a result of the growth of AI in finance. Part III considers the regulatory challenges of AI in the context of financial services and the tools available to address them, highlighting the necessity of human involvement. Part IV argues that the most effective path forward involves regulatory approaches which bring the human into the loop, enhancing *internal* governance and reducing financial supervision as *external* governance.

In the context of finance, the post-Crisis focus on personal and managerial responsibility systems provides a unique and important external framework to enhance internal responsibility in the context of AI, by putting a human-in-the-loop[10] through regulatory responsibility, as enhancements to the traditional three lines of defence, augmented in some cases with AI review panels.

We argue in Part V that this approach is central not only to addressing AI in finance but also potentially in any regulated industry which faces "black box" challenges in the context of AI or other new technologies.

I. AI and Finance

To consider AI in finance we first consider AI and its increasingly rapid development before turning to the particular characteristics of finance which make it highly suitable for AI and the range of uses which are rapidly evolving.

[9] For recent treatment, *see* Tom C.W. Lin, *Artificial Intelligence, Finance, and the Law*, 88 FORDH. L. REV. 531 (2019) (summarizing risks and limitations of AI in light of financial regulation).

[10] For a proposed Human-In-the-Loop framework, *see* Brian W Tang, "The Chiron Imperative – A Framework of Six Human-in-the-Loop Paradigms to Create Wise and Just AI-Human Centaurs" in Sophia Adams Bhatti, Susanne Chishti, Akber Datoo and Drago Indjic (ed), *The LEGALTECH Book: The Legal Technology Handbook for Investors, Entrepreneurs and Fintech Visionaries* (Wiley, forthcoming 2020).

A. AI and the Digitization of Everything

The term AI covers a series of technologies and approaches, ranging from "if-then" rule-based expert systems, to the interdisciplinary approach of combining linguistics and computer science known as natural language processing (NLP), as well as the marriage of algorithms and statistics known as machine learning that results in pattern recognition and inference from being trained from data rather than explicit human instructions. The increasing complexities of the latter seem to progressively reduce the role of humans as AI systems expand from supervised learning to unsupervised deep learning neural networks, reinforcement learning, collaborative learning, transfer learning and generative adversarial networks (GANs).

AI has been the focus of attention periodically over the past five decades. However, a unique confluence of factors has dramatically altered its developmental trajectory and as a result AI's evolution is raising an increasing range of issues, from the mundane to the existential.

There are five key factors which today empower the rapid development, training and evolution of AI: data, storage, communication, computing power, and analytics.

Rapid developments are noteworthy with regard to all of these factors: From the standpoint of data, the core aspect is digitization. It is only once data become available in digital form that the process of datafication – the application of analytics including AI – becomes effective. Thus, the "digitization of everything" at the heart of the Fourth Industrial Revolution is central to the rapid evolution of AI.[11] For datafication, the volume of data is important as well as its digitization: larger volumes of data are more effective in supporting datafication and in particular machine learning (ML) processes and the "training" of AI systems. Data storage, data storage quality and capacity have dramatically increased while costs have gone down. Thus, the volumes of data being digitally captured and stored now dwarf those captured and stored earlier. This combination of digitization and storage underpins datafication and AI.

Central to digital capture and storage are communications, with internet, mobile phones and the internet of things making it ever more possible to capture, store (locally and/or remoting), transfer, manipulate, and analyse data, increasingly on almost anything. With advances in computer vision, internet of things (IoT), analytics, and online and mobile penetration and usage, we can reasonably expect more and more data to be generated given that all these cloud connected devices have, compared to humans, effectively unlimited capacity to collect and store data.

Datafication also requires computing power and this has also increased dramatically, following Moore's Law, with dramatic reductions in cost. The emergence of quantum computing, if realised, will open incredible new avenues of processing. Datafication – while relying on computing power – also relies on research and development into algorithms and analytical processes themselves and this is another area of very rapid development.

This digitization of everything lies at the heart of the Fourth Industrial Revolution, ever-falling storage prices, telecommunications that link us all and to the cloud, ever-increasing computing power, and innovative algorithmic and analytical development underlies the explosion in datafication processes, which all in turn fuel AI growth that

[11] See Klaus Schwab, *The Fourth Industrial Revolution* (World Economic Forum, 2016).

looks set to continue, to the extent where discussions of the potential of the singularity are no longer the realm of science fiction.

B. AI and Digital Finance

These features come together uniquely in the contxt of finance.

After five decades of digital transformation, encompassing digitization and datafication, finance is the most globalized, digitized *and* datafied segment of the world's economy. While financial services have always integrated technical innovation,[12] this is particularly true for the latest wave of innovation referred to as financial technology (FinTech).

This process can be seen across four major axes: the emergence of global wholesale markets, an explosion of FinTech startups particularly since 2008, an unprecedented digital financial transformation in developing countries particularly China, and the increasing role of large technology companies (BigTech) in financial services (TechFin).

While finance and technology have always developed in tandem, since the 2008 Global Financial Crisis the changes have been unprecedented, particularly in terms of speed of change and range of new entrants including FinTech and BigTech firms. Speed of change can be seen particularly in the role of new technologies, often summarized under the ABCD framework: AI / analytics, blockchain, cloud and data, which are co-evolving at an increasing rate within finance. Many would also add mobile internet and IoT to these factors. Digital financial transformation combined with certain other aspects of finance make financial services particularly, and perhaps uniquely, fertile for AI development: these aspects include data, financial resources, human resources, and incentives.

As we have seen, one major technological pillar of digital financial transformation is the large-scale use of data: the financial sector has thus cultivated, over a long period, the extensive structured collection of many forms of data (e.g. stock prices). Such data have been standardized and digitized since the 1970s, with new forms of capture and collection constantly emerging. As a result, data in finance provides particularly fertile ground for AI, and finance provides the incentives and resources for the application of ever more sophisticated forms of analytics to ever wider ranges of data.

Furthermore, AI tends to perform best in rule-constrained environments, such as games like chess or Go, where there are a finite – although perhaps very large – number of possibilities to achieve specified objectives. This is the environment in which AI seems to outperform humans with increasing rapidity. This environment exists in many aspects of finance, for instance stock market investment, where there are specific objectives (maximizing profit) and set parameters of action (the trading rules and regulatory system) combined with massive amounts of data. Add technological possibility, in terms of computing power and analytics, to the financial and human resources and incentives to use them and it is apparent why finance is already transforming so rapidly as a result of digitization and datafication, and why this is likely to increase with further development of AI.

---

[12] See Douglas W. Arner, Janos N. Barberis & Ross P. Buckley, "The Evolution of FinTech: A New Post-Crisis Paradigm?", 47(4) Georgetown Journal of International Law 1345, 1345-1393 (2016).

The latter three – financial resources, human resources and incentives are fairly obvious: financial intermediaries generate massive amounts of income for their stakeholders, including management, investors and employees. As a result, they attract some of the very best human resources into the industry. Those human and financial resources have very strong reasons to continually search for advantages and opportunities for profit and thus invest substantial amounts in research, analytics and technology, to such an extent that there is an entire academic field – finance – focusing exclusively on research in the area and with major teams at financial institutions, advisory firms and academic institutions heavily focused on continually developing better analytical models for finance and investment. Since the 1980s, this process has had a very strong quantitative focus, involving the application of analytics to financial and other forms of data, and it is in the area of data where finance is perhaps unique from the standpoint of AI.

While finance and technology have always developed in tandem, since the 2008 Global Financial Crisis the changes have been unprecedented, particularly in terms of speed of change and range of new entrants including FinTech and BigTech firms. As of today, not merely the quantitative hedge funds are using algorithms, computational power and alternative data sources in finance. Instead, digital transformation has now impacted every aspect of finance, almost everywhere in the world.

As a result of digitization and datafication, almost every aspect of finance provides a potential area for AI.

Due to ever-improving performance in data gathering, processing, and analytics, AI can be expected to increasingly affect all operational and internal control matters of financial intermediaries, from strategy setting,[13] to compliance,[14] to risk management and beyond.[15]

C. Finance Use Cases

Today, algorithms and AI in financial services are frequently recognized as being used on the front- or back-end of an increasing range of processes and functions in finance.[16]

These include:

(1) customer related processes

---

[13] *See* John Armour & Horst Eidenmüller, "Self-driving corporations?" European Corporate Governance Institute-Law Working Paper No. 475/2019, https://ssrn.com/abstract=3442447, at 15 (while "strategic questions considered at the C-suite level" are unlikely to justify machine learning analysis, given the insufficiency of available data, "external generic data can be used to assist in scenario planning.").

[14] *See* Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669, at 690-93, 701-02 (2010).

[15] *See* Saqib Aziz & Michael M. Dowling, *Machine Learning and AI for Risk Management*, *in* DISRUPTING FINANCE. PALGRAVE STUDIES IN DIGITAL BUSINESS & ENABLING TECHNOLOGIES 33 (Theo Lynn et al. eds., 2019).

[16] *See* e.g., Hong Kong Monetary Authority & PwC, *Reshaping Banking with Artificial Intelligence* (November 2019) <https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_on_AI.pdf> ; Bank of England and Financial Services Authority, *Machine Learning in UK financial services* (October 2019) <https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf>

- on-boarding customers – particulary retail – more quickly and with a better user experience through biometrics such as facial recognition[17]
- marketing of financial services to specific user groups[18]
- enhancing customer relationship management, e.g. by (1) delivering instant responses to credit applications, (2) offering faster and better affordability checks for mortgages, and (3) delivering client-specific services with enhanced information and data-driven analyses[19]

(2) operations and risk management

- supporting or applying statistical models, e.g. for the calculation of pay-outs[20]
- managing risk, in particular setting risk limits and conducting stress testing[21] and credit scoring[22]
- determining executive compensation[23]
- monitoring boards of director decision-making biases[24]

(3) trading and portfolio management:

- capital allocation[25]

---

[17] This is a core aspect of RegTech.

[18] *See* Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner & Janos N. Barberis, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, 14 N.Y.U. J. L. & BUS. 393, 425-430.

[19] *See* AI Accenture, supra n 4, p. 13, 15, 17 (providing the example of an AI steering the SME client to the best qualified relationship manager for the SME's needs, based on an analysis of the SME's cash-flow and risk figures, and informing the relationship manager on the needs and background of the SME, ensuring un-interrupted services and advice).

[20] *See* Buchanan, supra n 1, at p. 2 (stating that Fukoku Mutual Life Insurance uses IBM's Watson Explorer AI to calculate pay-outs).

[21] *See* Financial Stability Board, "Artificial intelligence and machine learning in financial services" (Nov. 2017) 16 <https://www.fsb.org/wp-content/uploads/P011117.pdf > (summarizing Ai-based risk management and stress testing, and stating that one global corporate and investment bank is using unsupervised learning algorithms in model validation).

[22] *See* Oliver Wyman & China Securities Credit Investment Company, *China Credit-tech Market Report: Technology-Driven Value Generation in Credit-Tech,* 2019 <https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2019/apr/china-credit-tech-market-report-4.pdf>

[23] U.S.-based Equilar Inc. uses available compensation disclosures, performance targets and performance data, to generate "pay-for-performance" scores that can be used to determine whether an executive is over- or under-paid relative to executives of similarly situated companies. *See e.g.* Equilar's patent application for its "Equilar Pay for Performance Score", U.S. Patent Office, Patent Application Publication, Pub. No. US 2013/0159067 A1, Pub. Date: 20 Jun. 2013 (detailing the algorithms and data sources used for calculating the score).

[24] Venture capital firm Deep Knowledge Ventures assigned a (sort of) board position to an AI dubbed VITAL. VITAL scans prospective companies' financing, performance, IP and previous funding rounds. Its task is to identify overhyped projects. *See* Press Release, Deep Knowledge Venture's Appoints Intelligent Investment Analysis Software VITAL as Board Member – Hong Kong Venture Capital Fund Appoints Machine Intelligence as Board Member, 13 May 2014, *available at* https://globenewswire.com/news-release/2014/05/13/635881/10081467/en/Deep-Knowledge-Venture-s-Appoints-Intelligent-Investment-Analysis-Software-VITAL-as-Board-Member.html.. For a scholarly discussion of VITAL, *see* Luca Enriques & Dirk Zetzsche, Corporate Technologies and the Tech Nirvana Fallacy, ECGI Law Working Paper 457/2019; Michal S. Gal, *Algorithmic Challenges to Autonomous Choice*, 25 MICH. TECH. L. REV. 59, 61 (2018); Mark Fenwick, Wulf A. Kaal & Erik P.M. Vermeulen, *The "Unmediated" and "Tech-Driven" Corporate Governance of Today's Winning Companies* 42 n114, TILEC Discussion Paper No. 2017-009 (2017).

[25] *See* FSB, supra n 21, at 15 (summarizing the efforts to employ AI for optimizing risk-weighted assets

- financial services robo-advice[26]
- algorithmic trading[27]

(4) payments and infrastructure

- replacing human agents with chatbots in client communication[28]
- combatting fraud[29]

(5) data security and monetization

- document data extraction, for strategic or risk management purposes[30]
- automated threat prevention, detection and response, in particular through cybersecurity solutions[31]

(6) regulatory and monetary oversight and compliance

- transaction monitoring[32]
- detecting and reporting compliance breaches, for instance with regard to insider trading and market abuse[33]
- AML and know-your-customer checks (KYC)[34]
- Macroeconomic adjustments and fine-tuning[35]

(RWA) and margin valuation adjustment (MVA)).

[26] *See* Kokfai Phoon & Francis Koh, Robo-Advisors and Wealth Management, The Journal of Alternative Investments Winter 2018, 20 (3) 79-94; Jill E. Fisch, Marion Labouré, John A. Turner, The Emergence of the Robo-advisor, PRC Policy Paper; Tom Baker & Benedict G.C. Dellaert, Regulating Robo Advice Across the Financial Services Industry, 103 Iowa L. Rev. 713 (2018).

[27] *See* Andrei A. Kirilenko & Andrew Lo, Moore's Law versus Murphy's Law: Algorithmic Trading and Its Discontents, 27:2 Journal of Economic Perspectives 51-72 (2013); for an overview of the EU Framework in Art. 17 MiFID II see Tilen ČUK & Arnaud Van Waeyenberge, "European Legal Framework for Algorithmic and High Frequency Trading (Mifid 2 and MAR): A Global Approach to Managing the Risks of the Modern Trading Paradigm", 9:1 Eur. J. of Risk Regulation 136-153 (2018).

[28] *See* Amy Zirkle, The Critical Role of Artificial Intelligence in Payments Tech, 27 May 2019, < https://www.fintechnews.org/the-crirital-role-of-artificial-inteliigence-in-payments-tech/>.

[29] *See* blog Bizety.com, 'PayPal Deep Learning Methods Against Fraud', 18 Oct. 2016 (describing Paypal's deep learning algorithms that analyze thousands of data points (e.g. IP address, buying history etc.) in real time in order to identity theft, phishing attacks etc., and arguing that Paypal's fraud rate with 0.32% is one of the lowest in financial services, compared 1.32% as financial industry standard, citing the Lexis Nexis True Costs of Fraud Study 2016).

[30] *See* Buchanan, supra n 1, at p. 2 (stating that UK PropTech2 start-up Leverton applies AI to automatically identify, extract and manage data from corporate documents such as rental leases); FSB, supra n 21, at 21 (summarizing the efforts to employ AI for macroeconomic surveillance an data quality assurance).

[31] *See* https://www.infosecurity-magazine.com/next-gen-infosec/ai-future-cybersecurity/.

[32] *See* supra n. 29

[33] *See* FSB, supra n 21, at 19 (summarizing the efforts to employ AI for compliance and RegTech, and stating that one global corporate and investment bank is using unsupervised learning algorithms in model validation).

[34] *See* FSB, supra n 21, at 20 (stating that AI supports KYC checks primarily in two ways: "(1) evaluating whether images in identifying documents match one another, and (2) calculating risk scores on which firms determine which individuals or applications need to receive additional scrutiny. Machine learning-based risk scores are also used in ongoing periodic checks based on public and other data sources, such as police registers of offenders and social media services. Use of these sources may enable risk and trust to be assessed quickly and often cheaply. Firms can use risk scores on the probability of customers raising "red flags" on KYC checks.").

[35] *See* Okiriza Wibisono, Hidayah Dhini Ari, Anggraini Widjanarti, Alvin Andhika Zulen & Bruno

The adoption rate of AI and autonomous systems in finance is increasing rapidly. At the same time, the pain from skyrocketing compliance costs and sanctioning has induced financial institutions – from FinTech startups to global systemically important banks – to focus on back-office AI-solutions, in the form of RegTech. RegTech solutions include Amazon Alexa-like voice bots used by Credit Suisse for compliance queries[36], and bots at JP Morgan to review commercial loan contracts equivalent to 360,000 hours of work each year by lawyers and loan officers.[37] AI is also being applied to equities trade execution for maximum speed at best price at JP Morgan[38] and post-trade allocation requests at UBS[39], and to calculate policy payouts at Japan's Fukoku Mutual Life Insurance.[40] AI is also behind the trend to seek alternative data for investment decisions,[41] prompting the mantra "all data is credit data".[42]

D. A New Focus for Financial Regulators

In recent years regulators and policymakers have begun to consider the use of AI in finance.[43]

For instance, a World Economic Forum (WEF) report from August 2018[44] highlighted that the use of AI-enabled systems by financial institutions is promoting "new efficiencies" and delivering "new kinds of value". However, a tight focus on these new capabilities risked overlooking how financial services are shifting fundamentally, as financial institutions become "more specialized, leaner, highly networked and dependent on the capabilities of a variety of technology players."[45] Financial institutions need to develop new approaches to how they deal with their people, processes and data.[46] In this regard, the WEF suggests that collaboration amongst multiple stakeholders will be required to counter the potential social and economic risks

---

Tissot, The use of big data analytics and artificial intelligence in central banking, IFC Bulletin May 2019, <https://www.bis.org/ifc/publ/ifcb50.pdf>.

[36] "Credit Suisse has deployed 20 robots within bank, markets CEO says" (Reuters, 2 May 2017): <https://www.reuters.com/article/us-milken-conference-creditsuisse/credit-suisse-has-deployed-20-robots-within-bank-markets-ceo-says-idUSKBN17X2JC>.

[37] "JPMorgan Software Does in Seconds What Took Lawyers 360,000 Hours" (Bloomberg, 28 Feb. 2017): <https://www.bloomberg.com/news/articles/2017-02-28/jpmorgan-marshals-an-army-of-developers-to-automate-high-finance>.

[38]"JPMorgan develops robot to execute trades" (Financial Times, 31 Jul. 2017): https://www.ft.com/content/16b8ffb6-7161-11e7-aca6c6bd07df1a3c?mhq5j=e6

[39]"Robots enter investment banks' trading floors" (Financial Times, 6 Jul. 2017): <https://www.ft.com/content/da7e3ec2-6246-11e7-88140ac7eb84e5f1?mhq5j=e6>

[40] "This Japanese Company Is Replacing Its Staff With Artificial Intelligence" (Fortune, 6 Jan. 2017): <http://fortune.com/2017/01/06/japan-artificial-intelligenceinsurance-company/>

[41]"AI and Alternative Data: A Burgeoning Arms Race" (20 Jun. 2017): <https://www.waterstechnology.com/trading-technologies-andstrategies/3389631/ai-and-alternative-data-a-burgeoning-armsrace>

[42] *See* M. Hurley and J. Adebayo, "Credit Scoring In the Era of Big Data" 18:1 Yale Journal of Law and Technology: <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?Art.=1122&contex t=yjolt >

[43] We discuss a range of others in the following sections.

[44] World Economic Forum, "The new physics of financial services: How artificial intelligence is transforming the financial ecosystem" (15 Aug. 2018) < https://www.weforum.org/reports/the-new-physics-of-financial-services-how-artificial-intelligence-is-transforming-the-financial-ecosystem>.

[45] WEF, supra n. 44, at 19.

[46] AI Accenture, supra n. 4, at 5-7.

accompanied by the use of AI-enabled systems in finance.[47] Similarly, in October 2019, the WEF addressed how the financial services industry can responsibly use AI, focusing on understanding the governance requirements and risks of using AI in financial services. In particular, AI explainability, systemic risk and AI, bias and fairness, the algorithmic fiduciary, and algorithmic collusion are considered as prominent sources of uncertainties and risks associated with the use of AI in financial services. In the main, the WEF was of the view that in developing AI, the strategy taken should focus on a willingness to consider new governance and regulatory approaches that take into account the complex nature of AI-enabled systems, rather than developing "new ethics" for the financial services industry.

Among regulators, the European Central Bank has focused on the matter since at least 2017[48] and announced in February 2019 that algorithmic trading, an early and leading use case of AI, "has been growing steadily since the early 2000s and, in some markets, is already used for around 70% of total orders."[49]

In October 2019, the Bank of England and UK Financial Conduct Authority (FCA) released a major survey looking at maching learning (ML) in the UK financial industry.[50] Based on responses from 106 regulated financial institutions, the key findings included:

- ML is increasingly being used in UK financial services, with two thirds of respondents reporting they already use it in some form.
- Deployment is most advanced in the banking and insurance sectors.
- ML is now used across a range of business areas from front-office to back-office, and is used most commonly in AML and fraud detection as well as in customer services and marketing, with some firms also using it in areas such as credit risk management, trade pricing and execution, and general insurance pricing and underwriting.
- Regulation is not seen as a major barrier – rather, the biggest constraints are legacy IT systems and data limitations.
- Firms thought that ML does not necessarily create new risks, but could be an amplifier of existing ones. Such risks, for instance ML applications not working as intended, may occur if model validation and governance frameworks do not keep pace with technological developments.
- Firms validate ML applications before and after deployment. The most common validation methods are outcome-focused monitoring and testing against benchmarks.
- Firms use a variety of safeguards to manage the risks associated with ML. The most common safeguards are alert systems and so-called "human-in-the-loop" mechanisms. These can be useful for flagging if the model does not work as

[47] WEF, supra n. 44. *See also* UK Finance, supra n. 2.

[48] We discuss the Joint Report of the European Supervisory Authorities on the use of Big Data in Financial Services from March 2018 *infra*, at II.C.

[49] European Central Bank, "Algorithmic trading: trends and existing regulation", Newsletter 13 Feb. 2019, https://www.bankingsupervision.europa.eu/press/publications/newsletter/2019/html/ssm.nl190213_5.en.html >.

[50] Bank of England & Financial Conduct Authority, Machine Learning in UK Financial Services (Oct. 2019): https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf.

intended (e.g. in the case of model drift, which can occur as ML applications are continuously updated and make decisions that are outside their original parameters).

- Firms mostly design and develop ML applications in-house. However, they sometimes rely on third-party providers for the underlying platforms and infrastructure, such as cloud computing.
- The majority of users apply their existing model risk management framework to ML applications and many highlight that these frameworks might have to evolve in line with increasing maturity and sophistication of ML techniques.

A 2019 survey by the Hong Kong Monetary Authority[51] and accounting firm PWC among the HK banking industry highlighted that:

- 89% of respondents (authorised banks) had adopted or planned to adopt AI applications.
- 92% of respondents planned to significantly expand their AI workforce in the next 5 years.
- Total capital investment in the area will rise by 70% in the next 5 years.
- The top 5 use cases include cybersecurity applications, client-facing chatbots, remote onboarding, biometric customer identification and personalised advertisements.
- 95% of the banks tend to partner with external technology firms for AI implementation, while 82% managed the research and development stage internally.
- The top three reasons for utilizing AI included improving customer experience, enhancing risk management and reducing costs.
- The major impediments for AI use in finance, include: lack of employees with AI expertise (70%), insufficient data (52%), design ethics of AI (48%), data privacy and security (44%) and legal and compliance challenges (44%).
- The top three risks identified were: (1) lack of expertise among employees, (2) biased decisions made by the AI models, and (3) lack of quality data.

Clearly, AI is playing an increasingly significant role in finance, a role which is set to increase. Looking forward, does this raise potential financial regulatory concerns?

II. The Risks of AI in Finance

AI raises many questions that are yet to be answered. General concerns without a particular financial services dimension, that could yet impact financial services, include for instance: (1) what happens to workers whose jobs are replaced by AI?, (2) how do we distribute the wealth created by machines in our societies and across borders?, (3) how does humankind maintain control of super-human AI systems?, and (4) which rights do we assign to robots, i.e. are we willing to grant robots human-like rights?[52] These macro issues with AI have a very important role in the financial sector and potentially in regulation, as we consider how we wish finance, the economy and our

[51] See Hong Kong Monetary Authority & PWC, Artificial Intelligence (AI) in Retail Banking (November 2019). < https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Artificial_Intelligence_(AI)_in_Retail_Banking.pdf>.

[52] *See* Mirjana Stankovich et al, *Exploring Legal, Ethical and Policy Implications of Artificial Intelligence* (Sep. 2017).

societies to evolve as a result of the Fourth Industrial Revolution. These issues are central to discussions about AI and AI governance, within which finance plays an important role.

Our focus here however is on the more "micro" issues arising in the context of AI in finance. In particular, there is increasing awareness and analysis of the issues of fairness (including algorithmic bias), accountability and transparency (including "explainability") (sometimes summarized as "FAT") that arise with the implementation and evolution of AI.[53] These sorts of risks arise in particular as a result of "black box" issues: the view that AI develops independently and therefore its results are impossible to understand or accurately predict, highlighting the challenges of removing humans from AI systems.

In this section, we focus specifically on issues on the context of AI in finance from the standpoint of core financial regulatory objectives.[54] Using this lens of financial regulatory objectives, we categorize the major forms of risk as: data risks, cybersecurity risks, financial stability risks, and ethical risks.

Similar to the framework presented here, in December 2018, ACPR (Autorité de Contrôle Prudentiel et de Résolution – the French prudential regulatory authority within the Banque de France)[55] identified four major categories of risks associated with AI in finance:

(1) data processing risks associated with artificial intelligence;
(2) artificial intelligence and cybersecurity risks;
(3) the risk of players' dependency and the change of power relationships in the market; and
(4) challenges to financial stability and sovereignty.

ACPR further lists the governance and "explainability" of the algorithms, and challenges related to possible market restructuring, as further risks for supervisors.

The following sections consider these four major finance-related risks (data, cyber, financial stability, ethical) in light of the objectives of financial regulation.

---

[53] *See* eg, Brian W Tang, "Forging a Responsibility and Liability Framework in the AI Era for Regtech" in Janos Barberis, Douglas W Arner and Ross P Buckley, *The REGTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation* (Wiley, 2019), p 235; Yi Zeng, Enmeng Lu and Cunqing Huangfu, "Linking Artificial Intelligence Principles": <arXiv:1812.04814v1>; Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy and Madhulika Srikumar, "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI" (Berkan Klein Center Research Publication No.2020-1, 15 Jan. 2020): <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482## >

[54] The objectives of financial regulation can be summarized as: financial stability, financial efficiency, financial integrity, customer protection, economic development and financial inclusion. Financial stability can be seen both negatively (as avoidance of crises) and positively (as appropriate functioning of the financial system). Financial integrity focuses on prevention of criminal activities and use of the financial markets for activities like money laundering and terrorist financing. Customer protection focuses on systems to prevent abuses of consumers. Financial efficiency, economic development and financial inclusion focus on how to support the positive functioning and role of the financial system. See Douglas W. Arner, *Financial Stability, Economic Growth and the Role of Law* (Cambridge University Press, 2007).

[55] ACPR, "Artificial Intelligence: Challenges for the Financial Centre" (Dec. 2018): <https://acpr.banque-france.fr/sites/default/files/medias/documents/2018_12_20_intelligence_artificielle_en.pdf>

A. Data Risks

Central to the potential of AI is its potential to process far more data than humans, and without two human weaknesses. First, AI treats past data with the same precision as more recent data; in contrast, humans tend to treat more recent data as more significant and neglect older data in line with declining memory. Second, AI, if correctly programmed, subjects all data to the same objective treatment, while humans tend to discriminate among certain datapoints based on their experience, values and other non-rational judgement patterns. In this limited sense that technology does not follow its own agenda, and is not itself subject to humans' cognitive biases, technology can be said to be unbiased.[56] As we discuss below, however, the results can still be objectionable, resulting in bias in treatment.

AI use is subject to a number of risks and idiosyncratically suffers from a number of deficiencies.

1. Data dependency

AI is data dependent. The results of AI use are only as good as the data with which the AI has worked. Data dependency can give rise to a number of deficiencies.

First, even with a wide range of data generated in diverse ways, the data pool analysed **may lack the data relevant for the task**.[57] As a principle, past data may have some predictive capacity, in the sense that one event is more likely than another, but lack the ability to determine, strictly speaking, the path of future events in detail. Probability must not be confused with certainty. As the value of high-quality information and the threats posed by information gaps both continue to grow, regulators should focus on the development of widely used and well-designed data standards.[58]

Second, the **data quality may be poor**. An often-repeated example in the field of AI research includes the use of training data from the Enron case for compliance AI. From today's perspective, the Enron data are outdated. Even at the time, the Enron case was a deeply unfortunate outlier, rendering the use of the Enron dataset quite inappropriate.[59] From a legal perspective, protected factors come under threat if AI discriminates based on factors, proxies for these factors, or other factors altogether, that all describe little more than *a* part of social and financial relations within society. For instance an algorithm that determines creditworthiness based on consistency of phone use (rather than complete economic and financial data), may discriminate against members of certain religions who tend to use their phones far less on one day each week, such as a Friday or Saturday.[60]

Third, the **data used for AI analysis may suffer from biases**. This may be due either to data selection issues ("dashboard myopia") or data reflecting biases persisting in

---

[56] *See* Gramitto Ricci, "The technology and archaeology of corporate law", Cornell Law School research paper No. 18-40 (2018), at 37-38, http://ssrn.com/abstract=3232816; Martin Petrin, "Corporate Management in the Age of AI" (UCL Working Paper No.3/2019), at 34-35.

[57] Enriques & Zetzsche, supra n. 24, at 32.

[58] *See* Berner & Judge, "The Data Standardization Challenge", in Arner et al., Systemic Risk (2019), at 135-149.

[59] Enriques & Zetzsche, supra n. 24, at 31.

[60] *See* Zetzsche, Buckley, Arner & Barberis, *From FinTech to TechFin*, supra n 18.

society at large (e.g. that males are more likely to work in tech).[61] Decision-makers with prejudiced views may mask these by wittingly or unwittingly using biased data.[62] Biased data could likewise be selected in efforts to enhance an executive's personal bonus or to reduce oversight within an organization.[63]

2. Data availability

Data availability, even with a wide range of data generated in diverse ways, may be limited. The data may exist, but not be collected, structured or available for digital analysis. This may happen for two reasons. First, data collection is expensive. Small financial services providers may focus on the collection of data they believe valuable, giving life to their biases as to which data is relevant. Second, large financial services providers may be unwilling to share data they have with other firms, given that the other firms may either sell the data or become competitors of the data originator in the future[64] (the problem open banking is designed to address). The issue of data availability and accessibility then intersects with the vast world of data privacy and protection regulation.

3. AI Interdependency

A variant of the data availability issue is the lack of data on how other AI perform similar calculations at the same time, and how their decisions influence the tasks performed by the first AI. Such behaviour can result in "herding", in which actors make use of similar models to interpret signals from the market.[65] Algorithms trading in millisecond trading windows simultaneously in unexpected situations in which their operating assumptions do not apply have resulted in extreme volatility events, referred to as flash crashes.[66] This has resulted in regulation addressing algorithmic trading across the world.[67]

We can imagine similar problems with robo-advisors, in which one AI may front-run another AI advisor's recommendation. While risk management tools such as price limits and stop loss-commands (themselves algorithms) can mitigate *some* of the risks, these tools are costly and do not address all risks generated by multiple AI performing similar tasks, given the speed of events and that these algorithms will, again, be based on (sometimes) inadequate assumptions. Notwithstanding the former, the underlying issue remains that the original performance of calculations may turn out to be futile, or

---

[61] *See* Lin, supra n. 9, at 536-537.

[62] Solon Barocas & Andrew D Selbst, "Big Data's Disparate Impact" 104 CAL. L. REV. 671 (2016), at 692

[63] Enriques & Zetzsche, supra n. 24, at 30.

[64] Enriques & Zetzsche, supra n. 24, at 30.

[65] World Economic Forum, "Navigating uncharted waters: A roadmap to responsible innovation with AI in financial services" 62 (Oct. 23, 2019) < https://www.weforum.org/reports/navigating-uncharted-waters-a-roadmap-to-responsible-innovation-with-ai-in-financial-services>.

[66] *See*, Buchanan, supra n. 1, at 6. *See*, generally, on flash crashs Andrei A. Kirilenko, Albert S. Kyle, Mehrdad Samadi & Tugkan Tuzun, "The Flash Crash: High-Frequency Trading in an Electronic Market", 72:3 Journal of Finance 967 (2017).

[67] See references supra n. 27.

very harmful, whenever various algorithms perform and execute similar tasks simultaneously.

The alternative to uncoordinated behaviour, however, is more frightening: tacit collusion. If several self-learning algorithms find out that cooperation in capital markets is more profitable than competition, they could cooperate, i.e. manipulate information and prices to their own advantage. There is evidence for self-learning AI colluding in price setting,[68] and generally little reason to believe that multiple AI colluding in financial markets pricing is unlikely. The WEF has suggested financial institutions may potentially mitigate the risks of tacit collusion by (i) restricting their AI-enabled systems to communicate only with their own environments for "explicitly justifiable business purposes"; (ii) ensuring their AI-enabled systems' decisions are explainable by "valid, legal business reasons"; and (iii) requiring humans to oversee decisions made by AI-enabled systems.[69] These are all good suggestions, but may not always be sufficient to fully mitigate this substantial risk of AI interdependency, in particular if collaboration is profitable to the firm. Accordingly, it is not surprising that competition authorities in Europe and elsewhere are increasingly focussed on this issue of algorithms and collusion.[70]

B. Financial stability risks

The Financial Stability Board in 2017[71] analysed and summarized the possible financial stability implications of AI and ML as including the following:

- customer-focused uses – credit scoring, insurance and client-facing chatbots
- operations-focused uses – capital optimization, model risk management and market risk management
- trading and portfolio management – in trading execution and the scope of portfolio management
- regulatory compliance and supervision – applications by financial institutions for regulatory compliance (RegTech), uses for macroprudential surveillance and data quality assurance, uses and potential uses by central banks and prudential authorities (SupTech), and uses by market regulators for surveillance and fraud detection
- micro-financial analysis, including possible effects on financial markets, financial institutions, consumers and investors
- macro-financial analysis – market concentration and systemic risk importance of institutions, potential market vulnerabilities, networks and interconnectedness, and other implications.

---

[68] Ariel Ezrachi & Maurice E. Stucke, "Artificial intelligence & collusion: When computers inhibit competition" (2017) Univ. Ill. L. Rev. 1775.

[69] World Economic Forum, "Navigating uncharted waters", supra n. 69.

[70] *See* e.g., Bundeskartellamt and Autorite de la concurrence, *Algorithms and Competition* (November 2019) <https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_Working-Paper.pdf?__blob=publicationFile&v=5 >; UK Competition and Markets Authority, *Pricing algorihms: Economic working paper on the use of algorithms to facilitate colusion and personalised pricing* (8 Oct. 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf>

[71] *See* FSB, supra n. 21.

The FSB concluded that "AI and machine learning applications show substantial promise if their specific risks are properly managed". In terms of financial stability, the FSB stressed that "network effects and scalability of new technologies may in the future give rise to additional third-party dependencies" and this "could in turn lead to the emergence of new systemically important players," [72] up to the level of oligopoly or monopoly. Even more, some of these new market participants are currently unregulated and unsupervised. These third-party dependencies and interconnections could have systemic effects.[73] Further, the lack of interpretability or "auditability" of AI and ML methods has the potential to contribute to macroeconomic risk unless supervisors find way to supervise the AI. This is particularly challenging, given that "many of the models that result from the use of AI or machine learning techniques are difficult or impossible to interpret"[74] and AI-related expertise beyond those developing the AI is limited, in both the private sectors and among regulators.[75]

C. Cybersecurity

AI could be used to attack, manipulate, or otherwise harm an economy and threaten national security through its financial system directly and/or its impact on the wider economy.[76] For instance, algorithms could be manipulated in an effort to transfer wealth to foreign powers, to undermine an economy's growth in an effort to create unrest, or to send wrong signals to trading units to seek to trigger a systemic crisis.[77] The cybersecurity dimension is all the more serious given that many financial services firms rely on a small group of technology providers, that give rise, by themselves, to a new form of risk we have termed Tech Risk.[78] This is amplified by the fact that many AI-enabled systems have not been tested in financial crisis scenarios.[79]

The most important way to address cybersecurity is to (1) invest in cybersecurity resources, including in-house expertise and training of employees, and (2) have protocols in place to cooperate swiftly with other financial intermediaries in a similar situation, to ensure fast detection of, and responses to, these attacks, with or without involvement of regulators.[80]

D. Ethics and Financial Services

Ethics in finance are a crucial concern.[81] Ethical issues came to the fore in the wake of the Global Financial Crisis and have received continued attention as a result of

[72] *See* FSB, supra n. 21, at 33-34.
[73] For details *see* Lin, supra n. 9, at 544.
[74] *See* FSB, supra n. 21, at 33-34.
[75] *See* FSB, supra n. 21, at 33-34.
[76] For further examples *see* Lin, supra n. 9, at 538-539.
[77] *See* Ross P. Buckley, Douglas W. Arner, Dirk Zetzsche & Eriks Selga, *The Dark Side of Digital Financial Transformation: The New Risks of FinTech and the Rise of TechRisk*, __ SING. J. LEG. ST. __ (2020), *in press*.
[78] *See* Douglas W. Arner, Ross P. Buckley, and Dirk Zetzsche, "Fintech, Regtech and Systemic Risk: The Rise of Global Technology Risk", in Douglas W. Arner, Emilios Avgouleas, Danny Busch, and Steven L. Schwarcz (eds), *Systemic risk in the financial sector: Ten Tears after the great crash* (McGill-Queen's UP 2019), at 69.
[79] *See* Buchanan, supra n. 1.
[80] *See TechRisk*, supra n. 77.
[81] See earlier focus on this after the global financial crisis, eg, Brian Tang, "Promoting Capital Markets

subsequent scandals including those relating to LIBOR, foreign exchange and most recently the entire Australian financial system. A number of ethical questions with a particular financial services dimension will, most likely, be addressed by future (financial) legislation so as to make AI-driven financial services stable and sound, and their risks balanced. These tend to fall into four areas: AI as non-ethical actor, AI's influence on humans, artificial stupidity and artificial maleficence, and more general ethical considerations.

1. AI as nonethical actor

Algorithms do not "feel" or have "values". Training machines in values seems difficult, since we humans often lack insights into the human psyche: ie, humans often cannot tell why they feel as they do in certain ways.[82] While some ethical concerns, such as the ban of interest under Shariah law, can possibly be codified in ways that could be adopted by algorithms, most human feelings are more subtle, and subject to change under specific circumstances, reflecting the human abilities to learn and adapt.

AI's lack of ethical foundation could create serious harm for the portfolio value of a given financial intermediary if the AI misprices reputational risk. For instance, Microsoft's AI bot, Tay, "originally designed to interact with people online through casual and playful conversation, ended up hoovering good, bad, and ugly interactions. Within 16 hours of launch, Tay turned into a brazen anti-Semite, stating, 'Hitler was right'."[83] If a launched product came to this conclusion, we would expect serious stock price reactions. Unforeseen reputational risk can also prompt sudden and deeply unhelpful rule changes with major financial consequences. A vivid example is the near-prohibition of certain diesel cars in the EU following the diesel scandals in the US, contrary to the evidence that diesel's carbon emissions are lower than those of cars using petrol, and that its other pollution effects can be reduced even further by employing certain filters.[84] Volkswagen's severe ethical shortcomings in this case were all too human, but software controlling engine performance in test situations could foreseeably be programmed by AI at some point in the future.[85]

Professionalism: An Emerging Asian Model" , in Ross P Buckley, Emilios Avgouleas and Douglas W Arner, *Reconceptualising Global Finance and Its Regulation* (Cambridge University Press, 2016), at 357

[82] For details *see* Enriques & Zetzsche, "Corporate Technologies", supra n. 24, at 34.

[83] *See* Elle Hunt, "Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter" The Guardian (24 Mar. 2016) <https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter>; Dawson D & Schleiger E, Horton J, McLaughlin J, Robinson C∞, Quezada G, Scowcroft J, and Hajkowicz, (2019) Artificial Intelligence: Australia's Ethics Framework – Discussion Paper. Data61 CSIRO, Australia. < https://data61.csiro.au/en/Our-Research/Our-Work/AI-Framework>, at 31-32.

[84] European Environment Agency, "Explaining Road Transport Emissions: A Non-Technical Guide" (Jan. 2016) <https://www.eea.europa.eu/publications/explaining-road-transport-emissions>, p. 12; European Court of Auditors, "The EU's Response to the 'Dieselgate' Scandal", Briefing Paper (Feb. 2019) <https://www.eca.europa.eu/lists/ecadocuments/brp_vehicle_emissions/brp_vehicle_emissions_en.pdf >, [7] – [9].

[85] Capgemini Research Institute, "Accelerating Automotive's AI Transformation: How Driving AI Enterprise-wide Can Turbo-charge Organizational Value" 17-8 (Mar. 2019) <https://www.capgemini.com/wp-content/uploads/2019/03/Ai-in-automotive-research-report.pdf>.

The apparent risk is intensified by access to vast data accumulated on clients. The more data AI has about a certain person, the greater the risk of the AI nudging the human into certain behaviour, such as the purchase of an unsuitable financial product.

While some such unethical conduct could be mitigated through more diverse and broadly trained technical teams programming the AI, the core issue remains that the code itself is a non-ethical actor that does not necessarily constantly review, revise and reflect on its performance as we hope humans do.[86] AI needs human guidance for ethical decision-making: humans-in-the-loop are a necessity.

2. AI's influence on humans

Human-AI interaction will require particular analysis in financial services. If, for instance, humans respond differently to AI information requests than they would to human requests, paradigms on which financial services legislation is based may need rethinking. This could pertain, for instance, to (1) product governance and target market concepts, (2) mandatory disclosure, (3) mandatory client / consumer protection rules, and (4) choice of law and courts.

AI can enhance or diminish human capacity. One obvious field in which AI can enhance human capacity is knowledge and education. AI as "augmented intelligence" could turn an uneducated, unskilled human into a skilled investor, by way of recommendations or substitution for human decision-making. The same is true for human decision-making errors revealed in behavioural finance literature: AI could be programmed to address biases that reflect the human tendency to rely on patterns rather than thinking, given that the hard task of thinking could be outsourced to the AI. For instance, AI could adjust for the human bias to stick to investments made rather than opt for reconsiderations based on data.

On the other hand, AI could decrease human capacity. For instance, to the extent that the human need to develop advanced math and other sophisticated data analytical capacities is lessened with appropriate programmes being widely available, we would expect humans to develop lesser data analytic capacities in time. This is supported by the WEF which suggests that increasing reliance on AI in the future could lead to the erosion of "human financial talent" as humans lose the skills required to challenge AI-enabled systems or to respond to crises appropriately.[87] Our generally increasing lack of ability to remember telephone numbers or recall directions are vivid demonstrations of the effects of our increasing dependency on mobile phones today.

Both effects could be exploited in the financial services context. Coaching AI could be used to enhance financial and tech literacy of staff and investors, resulting in better resource allocation. Exploitative AI could ask clients to invest in overpriced, less valuable financial products that benefit only the product originator.

Obviously, the former can happen in a transparent or non-transparent, nudging manner. Research as to how humans respond to computer-generated incentives is ongoing and hints at serious risks for humans. Humans respond to certain communications with an enhanced degree of trust. AI can invest in relationships using an almost unlimited amount of resources, potentially generating a very high degree of trust. This illustrates

[86] *See further* Lin, supra n 9, at 537-538.

[87] World Economic Forum, "Navigating uncharted waters", supra n 69.

the level of responsibility AI developers bear, and the absolute necessity for ethical restrictions by way of rules and internal controls.

3. Artificial stupidity and artificial maleficence

How we can protect ourselves against AI mistakes and unethical behaviour is a major question. Errors and unethical behaviour can arise from poor or criminally motivated programming, or from inadequate datasets, or correlations with other events resulting in harmful unforeseen consequences. A common example given in AI literature refers to the task of eradicating cancer, for which a machine could propose the eradication of humankind. While human-controlled machines hopefully will not do this, in time, can we be so confident about super-human machines? We draw similar examples from financial services. For instance, where certain conduct results in liability and consumers sue far more than institutional clients, a computer could decide to avoid consumer relationships, thereby financially excluding consumers and depriving them of the opportunity to use the financial system to hedge against the risks of mankind, ranging from poor health to unemployment and old age.

E. Risk typology: Framework of analysis

The risks of AI for finance outlined in this section fall into three major categories. (1) information asymmetry, (2) data dependency and (3) interdependency.

First, as to information asymmetry, AI enhances information asymmetry about the true functions and limits of certain algorithms as third party vendor or in-house AI developers typically understand the algorithms far better than the financial institutions that acquire and use them (including the institutions' governance mechanisms) and the supervisors that supervise the institutions. This is to some extent the result of the innovation of new technology, but also egotistic and commercial considerations and other current "black box" technologies often mitigate against developers making the algorithms as transparent or as explainable as possible.

Second, AI enhances data dependency as data sources are critical for it to operate and AI assessed one day may change its operations, effects and potentially discriminating impact on a later day when using a different data pool.

Third, AI enhances interdependency in the sense that AI can interact with other AI with unexpected consequences, enhancing or diminishing its operations in finance.[88]

The law is likely to address the risks of AI generating undesirable results by preventive regulation or corrective liability allocation. Suffice to say that drafting these rules and enforcing them in light of the incredibly rapid developments in AI is a serious challenge. Leaving aside the much discussed private law dimension and liability allocation,[89] we will focus in the following Part on regulatory tools.

---

[88] *See* Lin, supra n. 9, at 542.

[89] *See* on AI-related liability from a U.S. perspective Mark A. Lemley & Bryan Casey, *Remedies for Robots*, 86 U. CHI. L. REV. 1313 (2019) (suggesting to focus on on no-fault liability systems, or at least ones that define fault differently, to compensate plaintiffs for AI-inflicted harm); Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571, 601–11 (2011) (proposing liability for open-source robots aiming at balancing the goals of fostering innovation and incentivizing safety); Rebecca Crootof, *War Torts: Accountability for Autonomous Weapons*, 164 U. PA. L. REV. 1347, 1389–1402 (2016) (discussing

III. Regulating AI in Finance: Challenges for External and Internal Governance

Markets and regulators have a number of means to address risks relating to financial services, ranging from private ordering and self-regulation to soft law approaches including recommendations to top-down command-and-control regulation. Financial supervision will be challenged by AI, requiring careful consideration of approaches which can best balance benefits and risks.

We begin with a discussion of the wide range of ethical frameworks which are being developed around the world to address the challenges of AI. Many of these however do not cater for the specific context of finance. We thus focus on approaches which are focusing specifically on AI in finance.

A. Ethical frameworks for AI

General frameworks addressing the question of the extent to which humans should be responsible when developing and dealing with AI are under development worldwide.[90] These clearly have direct relevance in the context of finance and financial regulation.

1. General frameworks

The UK House of Lords AI Select Committee defined five general principles of AI development and treatment in December 2017.[91] In April 2019, the European

robotic weapons systems and their potential legal liability); Karni A. Chagal-Feferkorn, *Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers*, 30 STAN. L. & POL'Y REV. 61 (2019); Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J. L. & TECH. 889, 931–32 (2018); from an European angle EUR. PARL., EUR. PARL. RES. SERV., PANEL FOR THE FUTURE OF SC. & TECHN., A GOVERNANCE FRAMEWORK FOR ALGORITHMIC ACCOUNTABILITY AND TRANSPARENCY 52, 72-74 (Apr. 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf (discussing no-fault/strict tort liability with varying degrees of liability depending on the transparency and criticality of the algorithmic systems and on AI certification by public authorities); as well as the contributions in LIABILITY FOR ARTIFICIAL INTELLIGENCE AND THE INTERNET OF THINGS (Sebastian Lohsse/ Reiner Schulze/ Dirk Staudenmayer, eds., 2019); Brian W Tang, "Forging a Responsibility and Liability Framework in the AI Era for Regtech" in Janos Barberis, Douglas W Arner and Ross P Buckley (ed), *The REGTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation* (Wiley, 2019), p 235.

Liability is also discussed in the context of liability for harm inflicted by autonomous vehicles, *see* Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 CAL. L. REV. 1611 (2017); Kenneth S. Abraham & Robert L. Rabin, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, 105 VA. L. REV. 127 (2019); Bryant Walker Smith, *Automated Driving and Product Liability*, 2017 MICH. ST. L. REV. 1; A. Michael Froomkin & P. Zak Colangelo, Self-Defense against Robots and Drones, 48 CONN. L. REV. 1 (2015)

[90] *See* https://blog.einstein.ai/frameworks-tool-kits-principles-and-oaths-oh-my/. For the Australian framework *see* Dawson et al., Artificial Intelligence: Australia's Ethics Framework, supra n 83. See also IEEE Global Initiative on Ethics of Autonomous and Intelligence Systems, whose Ethically Aligned Design <https://standards.ieee.org/industry-connections/ec/ead-v1.html >

[91] *See* House of Lords, Select Committee on Artificial Intelligence, "Written evidence volume: AI in the UK: ready, willing and able?" (11 Dec. 2017): https://www.parliament.uk/documents/lords-committee/Artificial-intelligence/AI-Written-Evidence-Volume.pdf. The five principles include the commitment (1) to serve and benefit humanity, (2) intelligibility and fairness, (3) data privacy and an

Commission released *Ethics guidelines for trustworthy AI*, based around seven key requirements: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; and accountability.[92]

Most influentially so far, in May 2019, dozens of countries including the United States adopted the OECD AI Recommendation, the first intergovernmental standard for AI:[93]

> "The Recommendation identifies five complementary values-based principles for the responsible stewardship of trustworthy AI:
>
> - AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being.
> - AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society.
> - There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them.
> - AI systems must function in a robust, secure and safe way throughout their life cycles and potential risks should be continually assessed and managed.
> - Organizations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles."
>
> "Consistent with these value-based principles, the OECD also provides five recommendations to governments:
>
> - Facilitate public and private investment in research & development to spur innovation in trustworthy AI.
> - Foster accessible AI ecosystems with digital infrastructure and technologies and mechanisms to share data and knowledge.
> - Ensure a policy environment that will open the way to deployment of trustworthy AI systems.
> - Empower people with the skills for AI and support workers for a fair transition.
> - Co-operate across borders and sectors to progress on responsible stewardship of trustworthy AI."

Drawing on the OECD AI Recommendation, the G20 endorsed the G20 AI Principles in July 2019.[94] In September 2019, endorsing the OECD Recommendations the US Chamber of Commerce released Principles on Artificial Intelligence,[95] including a call for US businesses to abide by these standards.

---

adequate level of data protection and against data monopolization, (4) to allow all humans to be educated and flourish mentally, emotionally and economically alongside AI, and (5) to avoid any AI's programming aiming at the destruction or deception of human beings.

[92] Independent High-Level Expert Group on Artificial Intelligence Set Up by the European Commission, "Ethics Guidelines for Trustworthy AI" (Apr. 2019): https://ec.europa.eu/digital-single-market/en/news/ethics-guidlines-trustworthy-ai.

[93] OECD Council Recommendation on Artificial Intelligence**,** https://www.oecd.org/going-digital/ai/principles/

[94] https://www.g20-insights.org/wp-content/uploads/2019/07/G20-Japan-AI-Principles.pdf.

[95] *See* https://www.uschamber.com/sites/default/files/chamber_ai_principles_-_general.pdf.

In the meantime, there are many parallel AI ethics initiatives arising from the private sector and researchers, such as the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems,[96] Future of Life Institute's Asilomar AI Principles[97], the Partnership on AI and the Montreal Declaration for responsible development of AI,[98] as well as a number of financial institutions.[99]

In China, the AI ethics initiatives have been more top-down, including the Beijing Academy of Artificial Intelligence's AI Principles in May 2019,[100] and the Ministry of Science and Technology National New Generation AI Governance Expert Committee's Governance Principles for a New Generation of AI in June 2019,[101] with increasing calls for cooperation over competition.[102]

2. Data protection and privacy

Data protection and privacy commissioners have increasingly viewed the governance of AI as within their purview. For instance, at the 40th International Conference of Data Protection and Privacy Commissioners in October 2018, the commissioners in their Declaration on Ethics and Data Protection in AI[103] endorsed six guiding principles as core values to preserve human rights in the development of AI:

(1) Fairness,
(2) Continued attention and vigilance, and accountability,
(3) AI system transparency and intelligibility,
(4) AI system responsible development and design by applying the principles of privacy by default and privacy by design,
(5) Empowerment of every individual, and
(6) Unlawful biases or discriminations arising from the use of data in artificial intelligence should be reduced and mitigated.

---

[96] See eg, IEEE Global Initiative on Ethics on Authomous and Intelligent Systems, *Ethically Aligned Design*: *A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*, Version II. (< https://standards.ieee.org/industry-connections/ec/autonomous-systems.html>

[97] Future of Life Institute, Asilomar AI Principles, 2017: < https://futureoflife.org/ai-principles/>

[98] Montreal Declaration for a responsible development of artificial intelligence (4 Dec. 2018) <https://www.montrealdeclaration-responsibleai.com/the-declaration>

[99] Institutions having adoped AI codes of conduct include, for instance, BNY Mellon, Deutsche Bank and Toronto Dominion.

[100] Beijing Academy of Artificial Intelligence (backed by the Chinese Ministry of Science and Technology and the Beijing municipality government) issued the Beijing AI Principles 28 May 2019: <https://www.baai.ac.cn/blog/beijing-ai-principles>

[101] Ministry of Science and Technology National New Generation Artificial Intelligence Governance Expert Committee, "Governance Principles for a New Generation of Artificial Intelligence: Develop Responsible Artificial Intelligence" (17 Jun. 2019) <http://most.gov.cn/kjbgz/201906/t20190617_147107.htm>: see China Daily English translation <https://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html>

[102] See e.g., New Economic Forum speech of China's former vice minister of foreign affairs Fu Ying, "Why the US should join China in Future-proofing AI Technologies", South China Morning Post, 5 Dec. 2019: <https://www.scmp.com/comment/opinion/article/3040435/why-us-should-join-china-future-proofing-ai-technology>

[103] "Declaration on Ethics and Data Protection in Artificial Intelligence", 40th International Conference of Data Protection and Privacy Commissioners in October 2018: <https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf>.

The Conference called for common governance principles on AI and a permanent working group on Ethics and Data Protection in AI to address the challenges of AI development.

Also relying on data protection principles, Article 22 of the European General Data Protection Regulation (GDPR) is seen as designed to require AI to perform ethically.[104] Entitled "Automated individual decision-making, including profiling", Article 22 states that a data subject has the right to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects her or him. Caveats apply if the decision is necessary for the entering into, or performance of, a contract between the data subject and the data controller; is authorized by the EU or a member state to which the controller is subject and which provides for suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; and is based on the data subject's explicit consent. Decisions should not be based on special categories of personal data unless suitable measures are applied to safeguard the data subject's rights and freedoms, and legitimate interests (see Article 9 GDPR). Where it is necessary for entering into or the performance of a contract, or where the data subject's consent is required, the data controller should institute suitable measures to safeguard the data subject's rights and freedoms, and legitimate interests. The data subject has the right to insist on human intervention on the part of the controller and to express his or her point of view to contest the decision.[105]

B. Financial Regulation and AI

Regulators globally have started to consider how AI impacts financial services and to issue regulatory guidance.

1. European Supervisory Authorities

In one of the first regulatory enquiries, in December 2016, the European Supervisory Authorities (ESAs) (European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA)) published a draft report on Big Data risks for the financial sector that included AI.[106] Of the 68 respondents, some stressed that "predictions based on Big Data can be flawed. It was also noted that [AI] could render the decision-making process less transparent and, in general, the intensity of the risks (…) could increase as a direct consequence of such new tools."[107] While most saw AI as an additional layer of Big Data analytics and a key tool to improve discovering patterns in data,

[104] *See* Jimmie Franklin, "GDPR has kept AI ethical, despite concerns" (IFLR, 2 Oct. 2019): https://www.iflr.com/Article/3896942/GDPR-has-kept-AI-ethical-despite-concerns.html.

[105] *See generally* Mirjana Stankovic el al, "Exploring Legal, Ethical and Policy Implications of Artificial Intelligence" Law, Justice and Development Draft White Paper (Oct. 2017).

[106] Joint Committee of the European Supervisory Authorities EBA, ESMA, EIOPA, Discussion Paper on the Use of Big Data by Financial Institutions, 19/12/2016, JC/2016/86.

[107] Joint Committee of the European Supervisory Authorities EBA, ESMA, EIOPA, Joint Committee Final Report on Big Data, JC/2018/0415 (Mar. 2018), <https://www.esma.europa.eu/sites/default/files/library/jc-2018-04_joint_committee_final_report_on_big_data.pdf>, at [50].

classification, evaluation and prediction, some stakeholders emphasized AI would add to the complexity, and incomprehensibility, of Big Data tools.[108]

The ESAs' final report in March 2018 found that, even when such techniques are used by financial institutions, in some respects "specific legislation in the field of data protection, cybersecurity and consumer protection is [best] positioned to address some of [AI] risks".[109] At the same time, the ESAs found that

> for the time being the current sectoral financial legislation sets requirements that are capable to address a number of risks specific to the use of Big Data techniques by financial institutions. Indeed a number of existing far reaching requirements, while not designed with the risks posed by the use of Big Data in mind, are applicable irrespective of the technological context.[110]

Given the ongoing implementation of legislation such as GDPR, the second Payment Services Directive (PSD2), the second Markets in Financial Instruments Directive (MiFID II) or the Insurance Distribution Directive, the ESAs refrained from recommending additional legislative steps, but focused on a data-oriented interpretation of existing sectoral legislation.

a. Organizational and prudential requirements

The ESA's interpretation focused, from organizational and prudential perspectives, on the following principles:

- Establishing and operating sound internal control mechanisms, effective procedures for risk assessment and effective control and safeguard arrangements for information processing systems.[111] The ESAs require financial institutions to allocate appropriate capital, human and IT resources to the implementation of Big Data from an operational standpoint.
- Ensuring continuity and regularity in the performance of their activities (and employing appropriate and proportionate systems, resources and procedures to this end).[112] The ESAs require that financial institutions address "the possible threats that may impact the continuity and the regularity of the performance of the financial institutions' activity."[113]
- Monitoring market activity and mitigating against counterparty or systemic risk or disorderly trading.[114] Investment firms and trading venues must ensure robust measures are in place to prevent algorithmic or high-frequency trading from disrupting the markets.
- Ensuring that reliance on a third party (i.e. outsourcing) does not impair the quality and the continuous performance of services.[115] The ESAs "stress that sectorial legislation requirements applicable to the outsourcing of important

[108] Joint Committee of the ESAs, supra n 107, at 98-99.

[109] Joint Committee of the ESAs, supra n 107, at p. 23.

[110] Joint Committee of the ESAs, supra n 107, at p. 23.

[111] Cf. Art. 16(5) MiFID II, Art. 18 Alternative Investment Fund Managers Directive (AIFMD), Art. 12 Undertakings for Collective Investment in Transferable Securities Directive (UCITS), Art. 5, 95 PSD2, Art.41, 44, 46 Solvency II.

[112] See Art. 16(4), 17 MiFID II, Art. 5, 95 PSD 2, Art. 41 Solvency II.

[113] Joint Committee of the ESAs, supra n 107, at p. 29.

[114] See Art. 17 MiFID II, Art. 79 CRD.

[115] See Art. 16 MiFID II, Art. 13 UCITSD, Art. 19(6) PSD II, Art. 38, 49 Solvency II.

functions of financial institutions do apply when an external provider is performing all or part of the outsourced functions through the use of (…) technologies."[116]

- Complying with record-keeping requirements,[117] given these requirements enable one to "reconstruct efficiently and evaluate the [tech] strategies/tools employed and ascertain compliance of financial institutions with all applicable regulatory requirements when providing services to consumers."[118]
- Taking steps to identify, prevent and manage conflicts of interests.[119] The ESAs acknowledge that the use of technology "can generate new contexts involving conflicts of interests, for instance from embedded biases or flaws in Big Data tools favoring firm's interests or certain clients over other clients."[120]

b. Business Principles

The ESAs further emphasize business principles requiring financial institutions to:

- Act honestly, fairly and professionally.[121] The ESAs insist that the "requirement to act fairly is of particular importance when the procedure or methodology being set-up or up-dated consists in the profiling of consumers."[122]
- Manufacture and distribute products and services which meet the needs of identified target clients and monitor such products.[123] Financial institutions should ensure that the use of data technologies to (i) identify target markets or (ii) assign a customer to a target market, is compliant with target market and product oversight requirements.
- Ensure that all information, including marketing communications, addressed by financial institutions to customers are fair, clear and not misleading.[124]
- Assess certain minimum, accurate and up-to-date, information about clients and products/services before providing certain services (e.g. suitability or appropriateness tests or creditworthiness assessments).[125]
- Preserve the interests of consumers when purchasing bundled or tied packages of products (in particular, client mobility and ability to make informed choices at the right time in the sales process):[126] "These provisions should prevent firms from using Big Data in order to promote bundled or tied packages of products

[116] Joint Committee of the ESAs, supra n 107, at p. 7.

[117] See Art. 17 MiFID II concerning algorithmic strategies. *See also* Art. 258(1)(i) Solvency II Delegated Regulation (EU) 2015/35, of Oct. 10, 2014. *See also* in the banking sector the Guidelines on outsourcing issued in Dec. 2006 by the Committee of European Banking Supervisors (CEBS) and the more recent Final Report of recommendations on outsourcing to cloud service providers published by the EBA in Dec. 2017.

[118] Joint Committee of the ESAs, supra n 107, at p. 30.

[119] Art 23 MiFID II, Art 17, 27, 28 IDD, Art 7 MCD. *See also* Art. 258(5) Solvency II Delegated Regulation (EU) 2015/35, of Oct. 10, 2014. *See also* EBA GL on product oversight and governance arrangements for retail banking products July 2015.

[120] Joint Committee of the ESAs, supra n 107, at p. 30.

[121] *See* Art. 24(1) MIFID II, Art. 17(1) IDD, Art. 7(1) MCD, Art. 12 AIFMD, Art. 14 UCITS.

[122] Joint Committee of the ESAs, supra n 107, at p. 30.

[123] Art. 16(3), 24(2) MiFID II, Art. 25 IDD, EBA GL on product oversight and governance requirements for manufactures and distributors of retail banking products, July 2015.

[124] *See* Art. 16 MiFID II, Art. 13 UCITS, Art. 19(6) PSD2*.

[125] *See* Art. 25 MiFID II, Art. 30 IDD, Art. 18, 20 MCD.

[126] *See* Art. 24(11) MiFID II, Art. 24 IDD, Art. 12 MCD, Art. 9 PAD, Art. 66, 67 of PSD.

which are not in the interests of clients."[127]

- Establish fair and efficient claims and complaints handling processes:[128] "This requirement is relevant to ensuring that Big Data analytics (e.g. tools enabling to predict more accurately whether a given consumer is likely or not to lodge a claim/complaint) do not lead to consumer detriment."[129]

c. Good practices

At the same time, the ESAs encourage the development and implementation of good practices with a view to "promoting a fair, transparent and non-discriminatory treatment of consumers and ensuring that Big Data strategies remain fully aligned with the interests of consumers."[130] Being summarized under somewhat loose headings, key aspects of good practices related to robust processes and algorithms, consumer protection and disclosures.

Demanding robust Big Data processes and algorithms, the ECB requires the "periodical monitoring of the functioning of Big Data procedures and methodologies as well as Big Data tools to adapt to technological developments and newly emerging risks".

Good practices pertaining to consumer protection require:

> - the "periodical assessment whether Big Data based products and services are aligned with consumers' interests and where relevant, the review and adjustment of the Big Data tools",
>
> - the "setting-up of procedures aimed at taking appropriate remedial actions when issues that may lead to consumer detriment materialize or are anticipated (notably in relation to the segmentation of consumers, e.g. impact on pricing or access of consumers to services due to increased segmentation of the target market)",
>
> - the factoring of "potential risks associated with the use of Big Data together with the content of the financial institution's Big Data transparency policy when designing and enforcing the financial institution's complaint handling framework",
>
> - the "adherence to and strict compliance with industry-specific codes of conduct under the GDPR",[131]
>
> - "special attention to their policy in terms of processing of data gathered from social media platforms considering the varied level of understanding by consumers of privacy settings on social media accounts and the risks of inaccuracies in such data", as well as
>
> - maintaining a balance between automated decision-making tools and human interventions.

---

[127] Joint Committee of the ESAs, supra n 107, at p. 31.

[128] *See* e.g. Art. 14 IDD, Art. 101 PSD2; Art. 26 MiFID II Delegated Regulation* requires firms to establish, implement and maintain effective and transparent procedures for the prompt handling of complaints.

[129] Joint Committee of the ESAs, supra n 107, at p. 32.

[130] Joint Committee of the ESAs, supra n 107, at p. 24.

[131] Financial institutions may choose to voluntarily join and adhere to approved codes of conduct or approved certification mechanisms, as an element to demonstrate compliance with GDPR (cf. Art. 24(3), 28(5), 40-43 GDPR).

Disclosure on the use of Big Data should ensure a high level of transparency towards customers concerning the use of Big Data technologies to process their data and promote "public awareness, consumer education on the phenomenon of big data and of consumers rights related to the use of Big Data by financial institutions."[132]

Remarkably, the ESAs did not stress two aspects of relevance to AI. First, the fact regulators may lack the means to monitor the limits of self-learning algorithms, and second, the role of senior management qualifications and responsibility. This will form the focus of the next sections.

2. Other Regulatory Approaches

An increasing range of other financial regulators are likewise engaging with AI. In chronological order:

- the Monetary Authority of Singapore introduced the new FEAT Principles to promote responsible use of AI and data analytics (considered below) in November 2018.[133]
- De Nederlandsche Bank issued principles for responsible use of AI, namely soundness, accountability, fairness, ethics, skills and transparency (or "SAFEST") in July 2019.[134]
- the WEF suggested in October 2019 that AI should be held to higher standards than humans and present systems as a result of the impact that AI can have on the financial services industry.[135]
- the HKMA issued its twelve "High-level Principles on Artificial Intelligence" in November 2019.[136]

a. Singapore

In November 2018, the Monetary Authority of Singapore (MAS) introduced the Principles to promote Fairness, Ethics, Accountability and Transparency (FEAT) in the use of AI and Data Analytics (AIDA) in decision-making in the provision of Singapore's Financial Sector[137]. These were updated in February, 2019 to reflect Singapore's Personal Data Protection Commission's Proposed AI Governance

---

[132] Joint Committee of the ESAs, supra n 107, at pp. 32-34.

[133] Monetary Authority of Singapore, "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector" (November 2018): https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf .

[134] De Nederlandsche Bank, "General Principles for Use of Artificial Intelligence in Finance" (25 Jul. 2019): https://www.dnb.nl/binaries/General%20principles%20for%20the%20use%20of%20Artificial%20Intelligence%20in%20the%20financial%20sector_tcm46-385055.pdf .

[135] World Economic Forum, "Navigating uncharted waters", supra n 69.

[136] Hong Kong Monetary Authority, "High-Level Principles on Artificial Intelligence" (1 Nov. 2019): <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf>.

[137] Monetary Authority of Singapore, "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector" < >. (12 Nov. 2018) <https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf > .

Framework[138] that had been issued in January 2019. The Proposed Model AI Governance Framework has two guiding principles, namely that organizations must ensure that decision-making using AI is explainable, transparent and fair, and that AI solutions should be human-centric. This Framework provides guidance in the following areas:

(1) Internal governance structures and measures,
(2) Appropriate AI decision-making models, including determining acceptable risk appetite and circumstances for human-in-the-loop, human-over-the-loop and human-out-of-the-loop approaches,
(3) Operations management, including good data accountability practices and minimizing inherent bias, and
(4) Customer relationship management, including disclosure, transparency, and explainability.

In November 2019, the MAS announced the creation of the Veritas framework to promote the responsible adoption of AIDA by financial institutions using open source tools as a verifiable way for financial institutions to incorporate the FEAT principles. With an initial consortium of 17 members, Veritas will initially focus on customer marketing, risk scoring and fraud detection.[139]

b. Hong Kong SAR

In Hong Kong, in May 2019, the HKMA encouraged[140] authorized institutions to adopt and implement Hong Kong's Office of the Privacy Commissioner for Personal Data's Ethical Accountability Framework for the collection and use of personal data,[141] and its Data Stewardship Accountability, Data Impact Assessments and Oversight Models that were introduced in October the prior year.[142]

In November, 2019, the HKMA's Banking Supervision department published its High-Level Principles on AI.[143] These Principles require that bank boards and senior management be accountable for the outcome of AI applications. In particular, the Principles reinforce that banks should:

(1) Possess sufficient expertise;
(2) Ensure appropriate level of explainability of AI applications;
(3) Use data of good quality;

---

[138] Singapore Personal Data Protection Commission, "A Proposed Artificial Intelligence Governance Model" (Jan. 2019) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/A-Proposed-Model-AI-Governance-Framework-January-2019.pdf>.

[139] Monetary Authority of Singapore, "MAS Partners Financial Industry to Create Framework for Responsible Use of AI" (13 Nov. 2019) <https://www.mas.gov.sg/news/media-releases/2019/mas-partners-financial-industry-to-create-framework-for-responsible-use-of-ai#1>

[140] Hong Kong Monetary Authority, "Use of Personal Data in Fintech Development" (3 May 2019) <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190503e1.pdf>

[141] Hong Kong Office of the Privacy Commissioner for Personal Data, Ethical Accountability Framework for the collection and use of personal data (24 Oct. 2018) <https://www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework.pdf>

[142] Hong Kong Office of the Privacy Commissioner for Personal Data, Data Stewardship Accountability, Data Impact Assessments and Oversight Models : Detailed Support for an Ethical Accountability Framework (24 Oct. 2018): <https://www.pcpd.org.hk/misc/files/Ethical_Accountability_Framework_Detailed_Support.pdf>

[143] Hong Kong Monetary Authority, "High-Level Principles on Artificial Intelligence" (1 Nov. 2019) <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf>

(4) Conduct rigorous model validation;
(5) Ensure auditability of AI applications;
(6) Implement effective management oversight of third-party vendors;
(7) Be ethical, fair and transparent;
(8) Conduct periodic reviews and on-going monitoring;
(9) Comply with data protection requirements;
(10) Implement effective cybersecurity measures; and
(11) Implement risk mitigation and contingency plans.

A few days later, the HKMA's Banking Conduct Department issued Guiding Principles on Consumer Protection in respect of Use of Big Data Analytics and AI (BDAI) by Authorized Institutions.[144] These guiding principles reinforced a risk-based approach to BDAI and focussed on four major areas, namely governance and accountability, fairness, transparency and disclosure, and data privacy and protection.

The HKMA's High-Level Principles on AI clearly set forth the expectation that "The board and senior management of banks should appreciate that they remain accountable for all AI-driven decisions", and that "the roles and responsibilities of the three lines of defence in developing and monitoring the operations of AI applications should be clearly defined."[145] This was reinforced in the HKMA's BDAI consumer protection guidance.[146]

C. Possible Regulatory Approaches

Current regulation focuses on human conduct, imposes safeguards on presumed static systems the vulnerabilities of which are not examined frequently, and entrenches peremptory transparency and auditability requirements.[147]

While designed as "high-level frameworks", the very fact that these guidelines have been issued by financial supervisory authorities turns these into more than mere "recommendations", into law *de facto*, if not in form: financial institutions subject to supervision will find it difficult to evade these supervisory expectations, with or without an authority's rule making capacity. This justifies a closer look at the measures available to financial supervisors in regulating AI.

In the following sections, we focus on five examples: authorization of AI itself, outsourcing rules and e-personhood, the qualifications of core personnel, the role of AI with regard to key functions, and sanctioning rules.

1. Authorization of AI

Enhanced use of AI influences the conditions for authorization. In particular, if a business model seeking authorization relies on AI, the business and operations plan

[144] Hong Kong Monetary Authority, "Consumer Protection in respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions" (5 Nov. 2019): <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191105e1.pdf>

[145] Hong Kong Monetary Authority, "High-Level Principles on Artificial Intelligence", supra n. 135, page 2 para 1.

[146] HKMA, supra n. 154, page 2: para 1: "The board and senior management of AIs should remain accountable for all the BDAI-driven decisions and processes."

[147] World Economic Forum, "Navigating uncharted waters", supra n 69.

must lay out both the functioning of the AI itself, and the client protection features, the regulatory capital assigned to financial and operational risks for the AI-performed services, and the back-up structure in case the AI fails. Regulatory frameworks around the globe currently already require IT contingency plans and multiple data storage and cybersecurity strategies. These regulatory approaches are unlikely to change fundamentally, but will become even more important in practice.

One potential response to AI-based threats discussed in the literature, however, is the introduction of a licensing requirement for AI being used by financial intermediaries.[148] Another potential response is a mandatory insurance scheme for AI.

Currently, financial services authorities worldwide are themselves increasingly seeking to upskill and introduce supervisory technology or suptech to perform meaningful reviews of AI. Software to monitor a self-learning AI's conduct does not, to our knowledge, yet exist, and outcome-based testing depends on the data pools available for testing; if the test pools differ from the real use case data pools the results of testing may be of little use.

AI authorization may also have a number of undesirable side-effects. The most important one is that authorization is potentially harmful for innovation given authorization is costly and takes time. It is also uncertain how rules could be drafted to reflect the daily reality of AI programming that minor amendments and improvements take place on almost a daily basis. Re-authorization of the code in this case will increase costs even further, meaning only AI with major income potential will be developed, and minor improvements of existing AI may well be uneconomic. Finally, in the case of self-learning AI, the actual authorized code will not be performing in practice, as the definition of self-learning AI is that it further develops its code while performing its services. Any authorization will thus be always outdated.[149] While sandboxes may in some settings be useful instruments for supporting innovation and effective regulation,[150] the authority can at best assess the services performed while the AI is functioning under sandbox conditions, thereby neglecting its performance under real conditions.[151] At the same time, fostering AI-related RegTech is independent of an AI's authorization (or sandbox, as the case may be); as it notably requires data-related reporting and governance rules.[152]

2. Regulatory outsourcing rules and e-personhood

In regulatory rulebooks around the world, crucial supplier frameworks apply if the AI is owned and operated by a separate services provider. If this is the case, the crucial supplier should be subject to additional monitoring by the outsourcing intermediary.

---

[148] *See* Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83 (2017).

[149] *See* Enriques & Zetzsche, "Corporate Technologies", supra n 24, at 56.

[150] World Economic Forum, "Navigating uncharted waters", supra n 69; RP Buckley, DW Arner, R Veidt & DA Zetzsche, "Building FinTech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond", *Washington University Journal of Law & Policy* (forthcoming 2020)*;* and DA Zetzsche, RP Buckley, DW Arner & JN Barberis, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation", (2017) (1) *Fordham Journal of Corporate & Financial Law* 31 (2017).

[151] *See* Enriques & Zetzsche, "Corporate Technologies", supra n 24, at 56.

[152] *See* Dirk Zetzsche, Douglas W. Arner, Ross P. Buckley, Rolf H. Weber, "The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II" , EBI Working Paper Series 2019/35, <https://ssrn.com/abstract=3359399 >.

The reality of much AI in financial services will, however, be that the AI is owned and operated in-house, by the financial intermediary's own staff. This prompts the question of the adequacy of the legal framework covering the AI.

One option for regulating in-house AI is the granting of limited legal personality to the algorithm itself, similar to a partial license, paired with minimum capital requirements. If the capital is depleted, for instance due to liabilities or regulatory sanctions, the algorithm needs to stop operations. The argument against such a limited e-personhood are similar to those against authorizing AI: The calculation of capital requires a clear delineation of risks created by the AI. If the limits of the function of the AI itself is in doubt, as is the case with regard to self-learning algorithms, regulatory capital will most likely be set too low or too high.

Further, authorities have less expensive ways to restrict the use of AI, even in the absence of an AI's own regulatory capital. These include imposing reporting requirements for AI-prompted damages upon intermediaries that employ AI, and responding to such reporting by issuing orders limiting, or prohibiting, the use of the AI.

3. AI as key function holder?

Another aspect of the fit and proper test refers to the use of AI as an executive or board member of the intermediary.[153] In this regard, legality and practical feasibility may be two different things. As to legality: in some jurisdictions executive functions can be assigned to legal entities, or the law is silent on the entity status of executives. In those jurisdictions, it may be lawful to appoint an AI as a board member, if necessary by embedding the AI as a SPV's sole activity. In other jurisdictions, these functions must be occupied by humans. As to practical feasibility, we could envision the AI functioning as a board member for certain routine tasks (the literature discusses the example of securitization vehicles in a corporate group), as well as for monitoring and supervisory services of a procedural nature, but would ask for a human board majority in order to ensure continuing operations when, and if, challenges exceed the limits of the programming of the AI.

Notwithstanding this, any rules allowing AI to assume some or all key functions of a financial intermediary must respect the existing limits of AI. This is particularly true for compliance monitoring. AI, on a stand-alone basis, is poorly adapted to handle compliance matters. The reason lies less in the lack of ethical screening abilities, and in the way rules are drafted: rules are incomplete on purpose. The law is full of vague terms such as "fair", "adequate", "just", "reasonable person" etc. These terms are used to ensure adjustment to an ever-changing world. Financial services are, however, a heavily regulated environment with plenty of rules and hence a lot of vagueness originates from these broad terms. These terms cannot be defined in 1/0 (yes/no) terms, and their meaning changes from context to context. If AI functioned as a compliance officer, we would thus expect inaccurate monitoring, widespread misreporting, and mispricing of risks all arising from vagueness in the law.[154]

[153] *See* note on VITAL *supra n* 24.

[154] *See* Enriques & Zetzsche, "Corporate Technologies", supra n 24, at 34-35.

4. Fit and Proper Test

One field where AI will most likely influence regulatory practice is the fit and proper test for key function holders (i.e. senior management or executives) as well as the board of directors. AI will impact existing licensing conditions in two respects. First, some existing requirements may be less necessary if an AI is doing the job. If in fact most decisions are taken by AI why should supervisors review a human executive's credentials?

Second, new requirements will reflect the greater reliance on AI, and some office holders may have new qualifications. For instance, EU authorities require executives of a financial intermediary to have at least three years of executive experience prior to appointment. This experience should demonstrate good standing, diligent handling of client matters and cooperation with the financial supervisory authority.

We have argued that there is little merit in reviewing AI itself in the context of AI authorization (*supra*, at III.B.4.); the same argument applies to assessing how fit and proper an AI may be. The increasing use of AI will, however, impact on the fit and proper test of humans functioning in AI-heavy financial institutions. This will almost certainly require modifications to existing regulatory approaches: AI experts may have accumulated their AI experience outside of the financial sector, for instance within a major e-commerce firm, given that technical innovation useful for financial services takes places in these firms. If financial supervisors insisted on their three year standard in financial firms, the supervised entities may find little tech expertise for hire. Authorities may need to modify their experience requirements for the financial sector, choosing to value high level AI experience in other sectors, so as to strengthen the firm's internal controls.

Given we believe senior management qualifications to be one of the most important regulatory tools in responding to the use of AI in financial services, we discuss these matters in more detail in the next part (IV.).

5. Sanctioning

Financial regulation imposes sanctions, some directed at at the institution's overall conduct and some others at staff member conduct. Usually, financial supervisors need to show some type of negligence or ill intent on the side of the financial institution in order to impose a sanction, with a deficiency of risk management system providing a fall-back option for sanctioning in case any harm has materialized. In the AI age, these cases will be increasingly hard to make. Where AI fails and even supervisors are incapable of establishing an AI's processes and limits with certainty; determining the culpability standard and burden of proof to be applied that will impose prudent sanctions while retaining incentives to innovate is going to be very difficult. After all, the nature of innovation is that innovations fail or do harm. Executives can do little more than select AI to the best of their abilities; where these abilities authorized under the fit and proper test fail potential sanctions may have exercised little steering effect, even if sanctions are possible under the broad "failure of risk management" rationale.

This brings us to the broadly discussed question of how to sanction an AI. Withholding compensation, naming and shaming, and financial penalties have little meaning for AI. In a similar vein, director disqualification, the equivalent of a "death penalty", as well as civil and criminal liability, provide limited steering effect for AI in the current form, unless the AI is programmed to have a desire to survive.

Hence, the sanctioning system must be reconsidered and include how to set proper incentives for the AI itself. AI-adapted financial regulation would possibly (i) require blame-free remediation in which organizations are able to learn from failures and make improvements, (ii) encourage forward-thinking collaboration between industry players to promote early detection and the avoidance of unexpected failures in AI systems, and (iii) employ fit-for-purpose explainability in which frameworks are utilised to decide "if" explainability is a requirement (thereby assisting organizations to prioritize their AI's objectives) and "how" explainability should be achieved given the wide range of AI use-cases.[155] Only where a conduct infringes said "if" and "how" rules would sanctions apply.

IV. Putting the Human-in-the-loop into Finance

While regulators expect financial institutions to deploy AI in a responsible manner and therefore develop and become accustomed to using new tools and solutions to safeguard the financial system,[156] we have shown that AI poses particular challenges from a regulatory standpoint: not all forms of financial services regulation are well-suited to ensuring the responsible use of AI, given the enhanced severity of information asymmetry, data dependency and interdependency.

In particular, given challenges of the "black box" problem in AI for regulatory and supervisory authorities, we argue in this section that measures focusing on personal responsibility requirements that put the "human-in-the-loop", should instead be the focus of regulating AI-enabled systems in finance.

Two particular approaches seem to be gaining increasing currency. The first involves the use of technology (including AI) to monitor staff behaviour and identify issues ideally before they arise (which should be seen as a form of RegTech). As we have argued elsewhere, we understand RegTech as logical consequence of enhancing Fintech; FinTech cannot work without proper RegTech in place. This is not the place to repeat this argument.

We thus turn to the second approach. This involves an increasing range of regulatory systems based on personal responsibility of designated senior managers for areas under their supervision – so-called "senior manager", "manager in charge", "key function holders" or "personal responsibility" systems. We argue that regulators should utilize and strengthen these external governance requirements in order to require "human-in-the-loop" systems for internal AI governance.

This approach builds on existing trends in financial regulation which have developed as a result of the Global Financial Crisis, LIBOR and forex scandals. These frameworks seek to produce cultural change and an ethical environment in financial institutions through personal responsibility of directors, management and, increasingly, individual managers.

We suggest that such personal responsibility frameworks should be supplemented to include responsibility for AI, including a non-waivable AI due diligence and explainability standard. Finally, we discuss particularities of an AI-adjusted personal

[155] *See* AI Accenture, supra n 4, at 18; UK Finance, supra n 2, at 10-13; World Economic Forum, "Unchartered Waters", supra n 65, at 21.

[156] World Economic Forum, "Navigating uncharted waters", supra n 65.

responsibility framework to ensure appropriate incentives. Such systems are particularly suited to "black box" issues but are also an effective approach for the range of major financial risks we identify in terms of data, cybersecurity, systemic risk, and ethics.

A. External Governance Requirements to Transform Internal Governance and Culture: Personal Responsibility Frameworks in Finance

Over the past decade, most major financial jurisdictions have imposed, or are in the process of imposing, director and manager responsibility frameworks through financial regulation. The EU has developed a framework for internal governance, the UK, Australia, and Hong Kong have implemented manager responsibility regimes, and Singapore and the US have proposed regimes.

1. European Union

The EU joint internal governance guidelines were published by the EBA and ESMA to build upon the Commission Delegated Regulation (EU) No 604/2014 criteria that identifies categories of staff whose professional activities have a material impact on a financial institution's risk profile. The joint internal governance guidelines aim to satisfy the CRD IV and MiFID II requirements and are made pursuant to Directive 2013/36/EU and Directive 2014/65/EU.[157]

The EBA and ESMA internal governance guidelines, and EIOPA's guidelines on systems of governance,[158] apply to all kinds of financial services institutions regulated under EU law, notably credit institutions, investment firms, managers of collective investment schemes, insurance undertakings and financial holding companies. These guidelines govern the conduct of the management body and key function holders. "Key function holders" is a term that refers to persons with significant influence over the direction of the institution that are not part of the management body. The management body and key function holders are to possess good repute, independence, honesty, integrity, knowledge, skills, and experience. Members of the management body must have sufficient time to perform their functions including understanding the business of the institution, its main risks, and the implications of the business and risk strategy.[159]

Responsibilities of the management body (in particular the CEO and other key executives) include setting, approving, and overseeing implementation of the overall

---

[157] These guidelines are to be read in conjunction with other guidelines and associated materials. See European Banking Authority, "Final Report - Guidelines on internal governance under Directive 2013/36/EU" (20 Sep. 2017) EBA/GL/2017/11, 5-7; "EBA and ESMA provide guidance to assess the suitability of management body members and key function holders" (26 Sep. 2017) <https://eba.europa.eu/eba-and-esma-provide-guidance-to-assess-the-suitability-of-management-body-members-and-key-function-holders>; Commission Delegated Regulation (EU) No 604/2014.

[158] EIOPA, Guidelines on Systems of Governance: <https://eiopa.europa.eu/GuidelinesSII/EIOPA_Guidelines_on_System_of_Governance_EN.pdf> (content-wise, these guidelines are essentially the same as the EBA and ESMA guidelines, only the older solvency framework for insurance undertakings from 2009 required a different wording.)

[159] European Banking Authority & European Securities and Markets Authority, "Guidelines on the assessment of the suitability of members of the management body and key function holders" (Mar. 21, 2018) ESMA71-99-598 EBA/GL/2017/12, 3 para 6, 5 para 3, 6, 11 para 26, 13 para 37, and 14 paras 39 and 41.

business strategy and the key legal and regulatory policies, the overall risk strategy, internal governance and control, risk capital, liquidity targets, remuneration policy, key functional holders' assessment policy, internal committees functionality, risk culture, corporate culture, conflict of interest policy, and the integrity of accounting and financial reporting systems.[160] The management body is also accountable for the implementation of the governance arrangements that ensure effective and prudential management of the institution, and promote the integrity of the market and the interests of clients.[161]

Key function holders such as heads of internal control functions including risk management, compliance and audit functions have a key role in ensuring that the institution adheres to its risk strategy, complies with legal and regulatory requirements, and ensures robust governance arrangements.[162] A sound and consistent risk culture is a critical element of risk management. Key function holders should know and understand the extent of risk appetite and risk capacity for their role and contribute to internal communications in relation to the institution's core values and expectations of staff. Effective communication should promote an environment of open communication, welcoming challenges in the decision-making processes, encouraging a broad range of views, allowing for the testing of current practices, stimulating a constructive critical attitude, and promoting an environment of open and constructive engagement throughout the entire organization.[163] The principal of proportionality applies to all governance arrangements, consistent with the individual risk profile and business model of the institution.[164]

2. United Kingdom: Senior Managers and Certification Regime

The UK's Senior Management regulatory regime evolved from the overall EU framework and has been highly influential internationally. Compliance with the regime is subject to firms and individuals being authorized by the UK Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA). Authorized firms are required to ensure that individuals who perform PRA-designated senior management functions are approved.[165] Authorization will not be granted unless the PRA and FCA are satisfied that the person meets the requirements of the Financial Services and Markets Act 2000 (FSMA).[166]

---

[160] European Banking Authority, "Final Report – Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU" (26 Sep. 2017) EBA/GL/2017/12, 18-20 para 23.

[161] European Banking Authority & European Securities and Markets Authority, "Guidelines on the assessment of the suitability of members of the management body and key function holders" (21 Mar. 2018) ESMA71-99-598 EBA/GL/2017/12, 6, 11 para 26, 13 para 37, 14 paras 39 and 41, and 31 para 110.

[162] European Banking Authority, "Final Report – Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU" (26 Sep. 2017) EBA/GL/2017/12, 11 para 33.

[163] European Banking Authority, "Final Report - Guidelines on internal governance under Directive 2013/36/EU" (20 Sep. 2017) EBA/GL/2017/11, 34 para 98.

[164] European Banking Authority & European Securities and Markets Authority, "Guidelines on the assessment of the suitability of members of the management body and key function holders" (21 Mar. 2018) ESMA71-99-598 EBA/GL/2017/12, 9 para 20.

[165] Pursuant to s. 59 of the Financial Services and Markets Act 2000.

[166] Conduct rules apply to the senior management functions specified by the PRA and FCA pursuant to s. 63 of the FSMA. See Bank of England, 'Senior Managers Regime: approvals'

Following the promulgation of the Commissioned Delegated Regulation (EU) No 604/2014, the PRA replaced the Approved Person Regime with the Senior Managers and Certification Regime (2016 SMCR) in March 2016. The 2016 SMCR is regulated by the PRA and the FCA and applies to all individuals who perform a "Senior Management Function" at banks, building societies, credit unions, and PRA-designated investment firms. The 2016 SMCR was expanded to cover insurance firms in November 2018, and expanded again, for FCA-regulated financial institutions, to apply to asset managers and designated activities of investment firms (Extended SMCR) from December 2019.[167]

The 2016 SMCR applies to UK deposit takers, PRA-designated investment firms, and UK branches of foreign banks. It is structured around: (1) a Senior Managers Regime for individuals who require regulatory approval (i.e. senior management functions and prescribed responsibilities); (2) a certification regime for regulated firms to assess the fitness and propriety of employees carrying out a "significant harm" function; and (3) conduct rules which apply to most bank employees.[168]

Senior managers are each required to have a clear and succinct statement of responsibilities. These include prescribed responsibilities listed by the regulator. Conduct rules for senior managers specify a "Duty of Responsibility" by taking "reasonable steps" to ensure that the business of the firm is controlled effectively and complies with the regulatory framework. Senior managers must take reasonable steps to ensure that any delegation of responsibility is assigned to an appropriate person and oversee an effective discharge of the delegated responsibility. A senior manager must disclose any information of which the PRA or FCA would reasonably expect notice.[169] The FCA has clearly expressed that the 2016 SMCR is not intended to subvert collective responsibility or collective decision-making.[170]

Conduct rules encourage a healthy culture whereby all financial services staff must act with integrity, due skill, care and diligence, openly cooperate with the PRA and FCA, pay due regard to the interests of customers and treat them fairly, and observe proper standards of market conduct. Firms are accountable for employee conduct and are required to notify the regulator of any breach of the conduct rules.[171]

The scope of the Extended SMCR is slightly wider than the 2016 SMCR. Senior managers are responsible for the firm's policies and procedures for countering financial crime risks: such as money laundering, sanctions, fraud, tax evasion and cybercrime; compliance with the Client Assets sourcebook where a firm has authority to hold client's money or assets; and, in terms of asset management firms, the value for money

<https://www.bankofengland.co.uk/prudential-regulation/authorisations/senior-managers-regime-approvals>.

[167] B. Reynolds, T. Donegan, S. Dodds & J. Adams, "The UK's Expanded Senior Managers and Certification Regime: Key Issues and Action Plan For Brokers, Advisors and Asset Managers" (8 Jul. 2019) Shearman & Sterling <https://www.shearman.com/perspectives/2019/07/the-uks-expanded-senior-managers-and-certification-regime-key-issues-and-action-pan>.

[168] Linklaters, 'SMCR for deposit takers and PRA-designated investment firms' <https://www.linklaters.com/en/insights/publications/smcr/smcr/smcr-for-deposit-takers-and-pra-designated-investment-firms>.

[169] KPMG, "Individual Accountability: Global regulatory developments in financial services" (July 2018), 4-5.

[170] Allen & Overy, "The UK Senior Managers and Certification Regime: Themes, trends and challenges from the first three years" (March 2019), at 17.

[171] Debevoise & Plimpton, "The UK's Senior Managers and Certification Regime" (18 Feb. 2019), para 4.1.

assessments, independent director representation, and acting in investors' best interests. This last point is applicable to managers of authorized (retail) funds.[172]

Ultimately, it is broadly recognized that these considerations also apply to the board,[173] where the need for upskilling similarly applies.

3. Australia: Banking Executive Accountability Regime

The Australian Prudential Regulation Authority (APRA) administers the Banking Executive Accounting Regime (BEAR).[174] Steps are being taken for Australian Securities and Investment Commission (ASIC) to co-regulate the BEAR obligations with APRA. Given ASIC is a conduct-based regulator, it appears well suited to regulate BEAR's conduct requirements.[175]

The BEAR came into effect on 1 July 2018 for large banks and 1 July 2019 for smaller banks (collectively, authorized deposit-taking institutions).[176] Both authorized deposit-taking institutions (ADIs) and individual accountable persons (IAPs) have responsibilities under BEAR. The ADI must provide individual accountability statements to APRA which clearly outline individual responsibilities and provide an accountability map outlining how accountability is allocated across an institution (based on size, risk profile, and complexity). IAPs are accountable for their actual or effective responsibilities for the management or control of a significant or substantial part, or aspect of, the ADI's operations or an ADI group. Specifically, IAPs have obligations to: act with honesty and integrity, and with due skill, care, and diligence; deal with APRA in an open, constructive, and co-operative way; and take reasonable steps in conducting their responsibilities to prevent matters arising that would adversely affect the ADI's prudential standing or prudential reputation.[177]

4. Hong Kong: Securities Firm Managers in Charge/Senior Management

In relation to Hong Kong securities firms, senior management are defined as directors and "responsible officers" of a corporation, and "Managers-in-Charge" (MICs). Licensed corporations are required to appoint an MIC as the person primarily responsible for each core function, overall management oversight, key business lines, operational control and review, risk management, finance and accounting, information technology, compliance, and AML/CFT. For each core function there should be at least

---

[172] ibid para 2.4.

[173] *See* e.g., Financial Conduct Authority, "Artificial Intelligence in the Boardroom" (Insight, 1 Aug. 2019) <https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf>

[174] BEAR is outlined in an information paper which recommends that it be read in conjunction with the requirements for accountability in Part IIAA of the Banking Act 1959, and an accompanying Revised Explanatory Memorandum. See APRA, "Information Paper: Implementing the Banking Executive Accountability Regime" (17 Oct. 2018), 4.

[175] ASIC, "ASIC update on implementation of Royal Commission recommendations" (19 Feb. 2019) <https://download.asic.gov.au/media/5011933/asic-update-on-implementation-of-royal-commission-recommendations.pdf>, 5 & 11.

[176] BEAR is set out in Part IIAA of the Banking Act 1959.

[177] APRA "Information Paper: Implementing the Banking Executive Accountability Regime" (17 Oct. 2018), sub-s 1.2.

one MIC responsible, although one MIC can manage several core functions (depending on the size and scale of the corporation's operations).

General Principle 9 of the "Code of Conduct for Persons Licensed or Registered with the SFC" (hereinafter, SFC Code of Conduct) states that senior management shall bear primary responsibility for ensuring the maintenance of appropriate standards of conduct and adherence to proper procedures by the firm. When determining responsibility in relation to a business operation, a person's actual and apparent authority shall be considered to determine responsibility and the degree of responsibility.[178] The Board shall approve and adopt a formal document clearly setting out, amongst other roles, responsibilities, accountability, and the reporting lines of senior management.[179]

Paragraph 14.1 of the SFC Code of Conduct specifies that senior management of a licensed corporation should properly manage the risks associated with the business of a corporation, including performing periodic evaluation of its risk processes, understanding the business nature of the corporation, its internal control procedures and its policy on the assumption of risk; and understanding the extent of their own authority and responsibilities.[180] Senior management are ultimately responsible for the adequacy and effectiveness of the corporation's internal control systems which include information management, compliance, audit or related reviews, operational controls, and risk management.[181] MICs should be aware of other codes and guidelines which impose responsibilities pursuant to section 193(3) of the Securities and Futures Ordinance (Cap. 571).[182]

5. United States: Proposed Senior Management Guidance for banks

In early 2018, the US Federal Reserve issued proposed senior management guidelines. The guidelines cover the senior management of large banks, bank-like institutions, and non-bank Systemically Important Financial Institutions (SIFIs). When the guidelines are formalized, they will build upon the independent risk management framework in Regulation YY which, in turn, implements certain provisions in sections 165 and 166 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.[183]

Senior management is defined as the core group of individuals directly accountable to the board of directors for the sound and prudent day-to-day management of the firm. For foreign-bank holding companies, senior management refers to those individuals inside or outside the US who are accountable to the intermediate holding-company board, US risk committee, or global board of directors with respect to their US operations.

Senior management are responsible for managing the day-to-day operations of the firm and ensuring safety and soundness, and compliance with laws, regulations (including consumer protection), and internal policies and procedures. The two key responsibilities of senior management are overseeing the activities of the firm's

178 SFC, 'Circular to Licensed Corporations Regarding Measures for Augmenting the Accountability of Senior Management' (Dec. 16, 2016), paras 1, 5, 7, 8, and 9.
179 ibid para 28.
180 ibid para 14(b).
181 ibid para 14 (c). Referring to the Internal Control Guidelines.
182 ibid para 14 (19).

183 Federal Reserve, "Proposed Supervisory Guidance" (11 Jan. 2018) [Docket No. OP-1594] 83 *Federal Register* 8, 1353 <https://www.govinfo.gov/content/pkg/FR-2018-01-11/pdf/2018-00294.pdf>.

business lines (individually or collectively); and the firm's independent risk management and system of internal control. There are additional responsibilities for certain senior managers, such as the chief risk officer in relation to independent risk management and the chief audit executive in relation to the internal audit function.

Senior management are responsible for maintaining and implementing an effective risk management framework and ensuring that risk is appropriately managed in a manner consistent with the firm's strategy and risk tolerance. Furthermore, senior management is responsible for promoting and enforcing prudent risk-taking behaviours and business practices. Senior management should periodically assess the firm's risk-management framework and ensure that the framework is comprehensive and appropriate for the firm's business lines and changes in economic and market conditions. Effective communication and information sharing should be maintained across the entire firm, including providing timely, useful, and accurate information to the board.[184]

6. Singapore: Proposed Senior Manager Guidelines

In June 2019, the MAS issued Proposed Guidelines on Individual Accountability and Conduct (IAC Proposed Guidelines). Senior managers are responsible for the day-to-day operations of a financial institution in Singapore.[185] The IAC Proposed Guidelines state that senior managers are responsible for the management and conduct of "core management functions" (CMFs), for the actions of their staff, and the conduct of the business.[186] Financial institutions should apply CMF definitions which reflect the actual responsibilities of a particular senior manager.[187] Responsibility is described as "principles-based" and therefore a list of mandatory responsibilities has not been issued.[188] MAS states that the level of responsibility should reflect the senior manager's roles in relation to the financial institution's Singaporean operations.[189] Senior managers are responsible regardless of their title or whether they are based overseas.[190] Material Risk Personnel are also covered by the IAC Proposed Guidelines.

B. Adressing the Knowledge Gap

The trend in financial services regulation appears clear: increasing personal responsibility for senior management and other individuals responsible for regulated activities within financial institutions. Such frameworks should also apply to AI.

We suggest that such personal responsibility frameworks provide the basis of an appropriate system to address issues arising from AI in finance, in particular the three challenges of AI (information asymmetry, data dependency and interdependency). We propose that manager responsibility framework need to be expanded to specifically incorporate responsibility for AI in regulated activities, thus mandating a "human-in-the-loop". This should be extended to specifically mandate due diligence and explainability requirements. Such an approach could be augmented in many cases through the addition of AI review committees. Such an approach is highly effective in

[184] Ibid.
[185] IAC Proposed Guidelines (6 Jun. 2019), para 3.3.
[186] ibid paras 1.1 & 3.1.
[187] ibid para 3.23. For a definition of CMFs in relation to Senior Management, see ibid Annex C, 50ff.
[188] ibid para 3.23.
[189] ibid para 2.25
[190] ibid para 3.5.

addressing black box issues but also in providing a framework to address the four core financial risks we identify relating to data, cybersecurity, systemic risk, and ethics.

1. AI review committees

In order to address the information asymmetry as to AI's functions and limits, regulators should take advantage of an important practice emerging in some non-financial companies. These companies have created independent AI review committees to provide cross-disciplinary and impartial expertise to such companies developing and utilising AI.[191] Some of these committees or boards have been quite impactful, such as Axon's management and board accepting the recommendation of its AI and Policing Ethics Board to impose a moratorium on the use of facial recognition in Axon's body cameras.[192] The impact of others have been less,[193] or remain to be seen.[194] In any case, these boards are designed to augment decision-making and do not detract from the ultimate responsibility vested in management and the board regarding AI governance.

2. AI Due Diligence

The second tool that reinforces and supports manager responsibility is mandatory AI due diligence. Due diligence is meant to include a full stock-taking of all characteristics of the AI. At a minimum this must include the AI explainability standard further described in the next section. AI due diligence is the standard prior to AI employment, while AI explainability is the standard to meet throughout the use of any AI.

In order to reflect data dependency one part of the due diligence is a mapping of the data sets used by the AI, including an analysis of data gaps and data quality.

AI due diligence is a result of individual responsibility systems: the necessity of the individual having performed sufficient due diligence in exercise of their responsibilities to avoid liability for any failures which arise, whether from internal governance systems, employees, third parties, or IT systems.

---

[191] See Brian W Tang, "Independent AI Ethics Committees and ESG Corporate Reporting on AI as emerging corporate and AI governance trends" in Ivana Bartoletti, Susanne Chishti, Anne Leslie and Shan M. Millie (ed), *The AI Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation* (Wiley, forthcoming 2020).

[192] See Rick Smith, "The Future of Face Matching at Axon and AI Ethics Board Report", Axon, (27 Jun. 2019) < https://global.axon.com/company/news/ai-ethics-board-report >/.

[193] See e.g., "Google Quietly Disbanded Another AI Review Board Following Disagreements", Wall Street Journal (16 Apr. 2019).

[194] See Facebook's new Oversight Board: "Establishing Structure and Governance For an Independent Oversight Board" (Facebook, 17 Sep. 2019) < https://about.fb.com/news/2019/09/oversight-board-structure/ >. Megvii Technology Limited, one of the first pure-play AI companies from China seeking to be listed, has set up an AI Ethics Committee: see Megvii Technology Limited, Application Proof filed with the Stock Exchange of Hong Kong, p.3 <https://www1.hkexnews.hk/app/sehk/2019/100283/documents/sehk19082500082.pdf>

3. AI Explainability

Explainability requirements are necessary as a minimum standard for humans-in-the-loop in AI use, i.e. demanding that the function, limits and risks of AI can be explained *to someone*, at a level of granularity that enables remanufacturing of the code.[195]

In principle, the someone should be the member of the executive board responsible for the AI (thus relying on the managers' incentive to avoid sanctions) or an external institution, in particular regulators, supervisors and courts.

We thus propose, in a first step, to introduce explainability requirements for the responsible managers; and a requirement that the explainability be documented. In a second step, supervisory authorities may review compliance with the explainability requirements. In this way manager responsibility systems will be buttressed by explainability systems which are in turn a necessary result of personal responsibility and accountability to regulators on an individual level for regulated functions. Individual managers will have to be able to explain their own decisions, the actions of their employees and contracts, and of their IT systems.

C. Personal Responsibility in Financial Regulation: Challenges in Building Human-in-the-Loop

A number of concerns must be considered in the context of promoting the personal responsibility model. These include: (1) the inability to control AI well by internal governance, (2) overdeterrence, and (3) how to deal with FinTech start-ups.

1. Inability to control autonomous AI internally

If AI cannot be controlled by external monitors, such as financial supervisory authorities, it could be argued that AI cannot be monitored effectively and kept under control by senior management not directly involved in AI coding and operations. In this case, key staff will lack control over the AI, just as will external supervisors.

Methods of internal control include, for instance, internal reporting, defining risk limits in terms of risk budgets, assigning budgets for code development and data pool acquisition, and setting adequate incentives through balanced compensation models. If key function holders / senior management are well aware of their responsibilities, in most cases these governance tools will be imposed with a view to controlling AI since the key managers' income expectation and future cash-flow opportunities depend on meeting their responsibility.

More importantly, personal responsibility / liability systems place the responsibility for areas of regulated conduct under the responsibility of specific individuals, thus meaning that an individual is directly responsible from a regulatory standpoint for regulatory breaches which arise in their area of responsibility. Thus, the individual will have strong incentive to monitor and understand their functional area, their staff, their third parties contractors and suppliers, IT systems. Once such understanding of responsibility develops, a culture of due diligence and explainability should evolve to address the "black box" problem. In cases where it does not, the individual and board will nonetheless remain responsible for developments.

[195] *See* on explainability World Economic Forum, "Navigating uncharted waters", supra n 69, at 32.

Naturally, the manager responsibility model requires including key people, for purposes of AI development, in the responsibility concept. Hence, key developers (to the extent the solution is developed internally) must be included in the net of responsibility. As we have argued in relation to TechRisk, an individual should also be designated with regulatory responsibility for IT and tech systems, for similar reasons and to achieve similar results.[196]

The manager responsibility concept may prove ineffective in two cases. First, if the developers lose control over self-learning AI, as can occur if, for instance, self-learning AI taps into unexpected data pools, and produces unexpected correlations. However, the production of unacceptable and unexpected outcomes can be countered by switching off the AI, an outcome which should be incentivised through personal responsibility requirements. Accordingly, given the risk of global systemic risk and impact on lives that finance plays, all AI used in finance should be programmed so as to be able to be switched off: the responsibility model should be designed to ensure that this indispensable requirement is in the code, and, most importantly, the organization needs to be able to function with the AI turned off. A contingency plan is vital and needs to include (a) the option to switch off the AI, and (b) the measures that will be instituted to deal with the consequences of doing so (such as manual, instead of algorithmic, trading, manual loan portfolio allocation, etc.).

Second, the responsibility concept fails if developers develop a super application that is so clever it can deceive human beings entirely by continuing to function even if developers activate the pre-programmed off switch. The sanctions for such a superapp behaving in this way must be so severe that developers have every incentive to ensure it is impossible. This does not mean that such a super app will never be built, but the manager responsibility concept should ensure even if it is developed outside of regulated financial services (such as through cloud service providers), that should be an important consideration in its adoption and implementation within regulated financial services.

2. Overdeterrence

Manager responsibility could be too much of a good thing. If the regulatory burden deters managers from being involved in AI-based financial services, we may find only reckless and unreflective people developing AI for financial services and serving as senior managers for financial services firms, resulting overall in weaker, rather than better, governance. Regulators must respond to this concern with proportionate responses to apparently irresponsible conduct including into human contributions to failure such as which person failed to perform the AI due diligence or bypassed the explainability requirements. An initial assessment will take place in the context of managerial requirements, including fitness and properness. Personal responsibility / liability systems should also include frameworks of continuing education as well as ongoing fit and proper requirements in order to balance this risk.

Facing the choice between individual and collective responsibility, individual responsibility concepts could lead to less diligence in monitoring fellow key function holders. Collective responsibility, by contrast, could increase monitoring among key function holders, but lead to overdeterrence. This debate is live amidst the blame allocation arising from the ongoing Westpac scandal in Australia that is being attributed

[196] See *TechRisk*, supra n. 77.

to a relatively low key piece of software that led to allegedly some 23 million AML breaches.[197] A compromise would include defining some collective core duties while also imposing individual responsibility. This is clearly the case in both board responsibilities as well as corporate responsibility, both thereby putting in place collective responsibility as well as individual responsibility systems of internal governance via external regulatory requirements.

3. FinTech start-ups

A third concern relates to FinTech start-ups. Usually, regulators require experience and management skills in finance as a precondition for licensing a financial entity. Start-up staff often have little experience in running a regulated firm. If regulators require this expertise of all key function holders, innovation will be severely impaired.

The obvious response is for regulators to require sufficient expertise *and* experience from the start-up's board and key executives, *as a group*. Under this whole board and executive concept, some board members and executives can contribute the IT / AI expertise while others contribute their experience in running a regulated financial services firm. After a certain time in the business, all board members and executives should be able to meet the standards for seasoned financial intermediaries.

For personal responsibility in given areas, specific area related expertise is required as one aspect of the fit and proper test. While it may make sense in a startup to take a balanced and proportionate approach to board and key executive requirements as a group, specific regulatorily mandated individual responsibility requirements, expertise and experience requirements would remain necessary as part of the licensing process.

V. Conclusion

The financial services industry is one of the leaders in the use and development of AI and going forward AI is likely to become an ever more important technology for financial services firms. However, AI comes with a number of very substantial technical, ethical and legal challenges that can undermine the objectives of financial regulation, from the standpoint of data, cybersecurity, systemic risk, and ethics, in particular in the context of black box issues.

As we have shown, traditional financial supervision focussed on external governance is generally unlikely to be highly effective in addressig the risks created by AI. This is because of three main regulatory challenges: (1) enhanced information asymmetry about the AI; (2) data dependency; and (3) interdependency with other AI. Accordingly, even where supervisory authorities have exceptional resources and expertise, supervising the use of AI in finance by traditional means of financial supervision is extremely challenging.

In order to address this weakness, we suggest that the internal governance of financial institutions be strengthened through imposing personal responsibility requirements to put a "human-in-the-loop", based on existing post-Crisis frameworks of managerial responsibility. These should ideally be cognisant of and consistent with broader data

[197] See Paul Smith, "Westpac's mess could happen to anyone" (Australian Financial Review, 6 Dec. 2019): < https://www.afr.com/technology/westpac-s-tech-mess-could-happen-to-anyone-20191204-p53gqq>.

privacy and human-in-the-loop approaches beyond finance.[198] From a financial authority's point of view, the strengthening of internal governance can be achieved, for the main part, through a renewed supervisory focus on senior managements' (or key function holders') personal responsibilities and accountability for regulated areas and activities for which they are designated responsible for regulatory purposes as well as key input from external AI experts and stakeholders. These key function holder rules, particularly if enhanced by specific due diligence and explainability requirements, will assist core staff of financial services firm to ensure that the AI under their control is performing in ways consistent with their personal responsibilities. If it is not, they will nonetheless be responsible. That is the nature of personal responsibility systems: the manager etc in charge is responsible for themselves, their area, their staff, their third party contractors, and their IT, including AI. This encourages – as a result of direct personal responsibility – due diligence in investigating new technologies, its uses and its impact and on requiring explainability systems as part of any AI system – or IT system for that matter. This is necessary from the standpoint of an individual who has potential direct responsibility in the event of a regulatory action for any failure: due diligence and explainability will be the key to a personal defence. Likewise, a similar approach would be incentivized in the context of regulatory use of AI: the necessity of defending any enforcement action in court requires due diligence in development and use of AI for regulatory purposes as well as explainability systems in order to defend their actions. While clearly effective in the black box context, this also addresses other data, cybersecurity, systemic risk, and ethical issues in the context of AI in finance, particularly when combined with centralized AI review committees to address issues of collective responsibility of the board and more broadly.

Importantly, this approach – while a natural evolution in the context of financial regulation – also has great potential for addressing AI concerns in other regulated industries through the regulatory requirement for "human-in-the-loop" personal human responsibility systems. While it does not necessarily address the macro issues which are emerging as a result of the Fourth Industrial Revolution, the digitization of everything, and AI, it does at least make sure that humans are centrally involved in the context of the evolution of AI in regulated industries, providing for personal understanding and responsibility to address many of the core micro issues, and puts us in a better position to understand the potential macro issues as they arise.

[198] See eg. Tang, *ibid*, n10.

Fintech Toolkit: Smart Regulatory and Market Approaches to Financial Technology Innovation

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

As a federally owned enterprise, GIZ supports the German Government in achieving its objectives in the field of international cooperation for sustainable development.

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn

Dag-Hammarskjöld-Weg 1-5
65760 Eschborn
Germany
T +49 61 96 79-0
F +49 61 96 79-11 15

E Atilla.yuecel@giz.de
I www.giz.de

On behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ).

Authors:
Dirk A. Zetzsche, Professor of Law, ADA Chair in Financial Law, University of Luxembourg

Douglas W. Arner, Kerry Holdings Professor in Law, University of Hong Kong

Ross P. Buckley, KPMG Law – King & Wood Mallesons Professor of Innovative Disruption, UNSW Sydney

The report benefitted from the inputs of Atilla Kaiser-Yücel and the commentary by Sofia Bublatzky and the Financial Systems Development MENA Working Group.

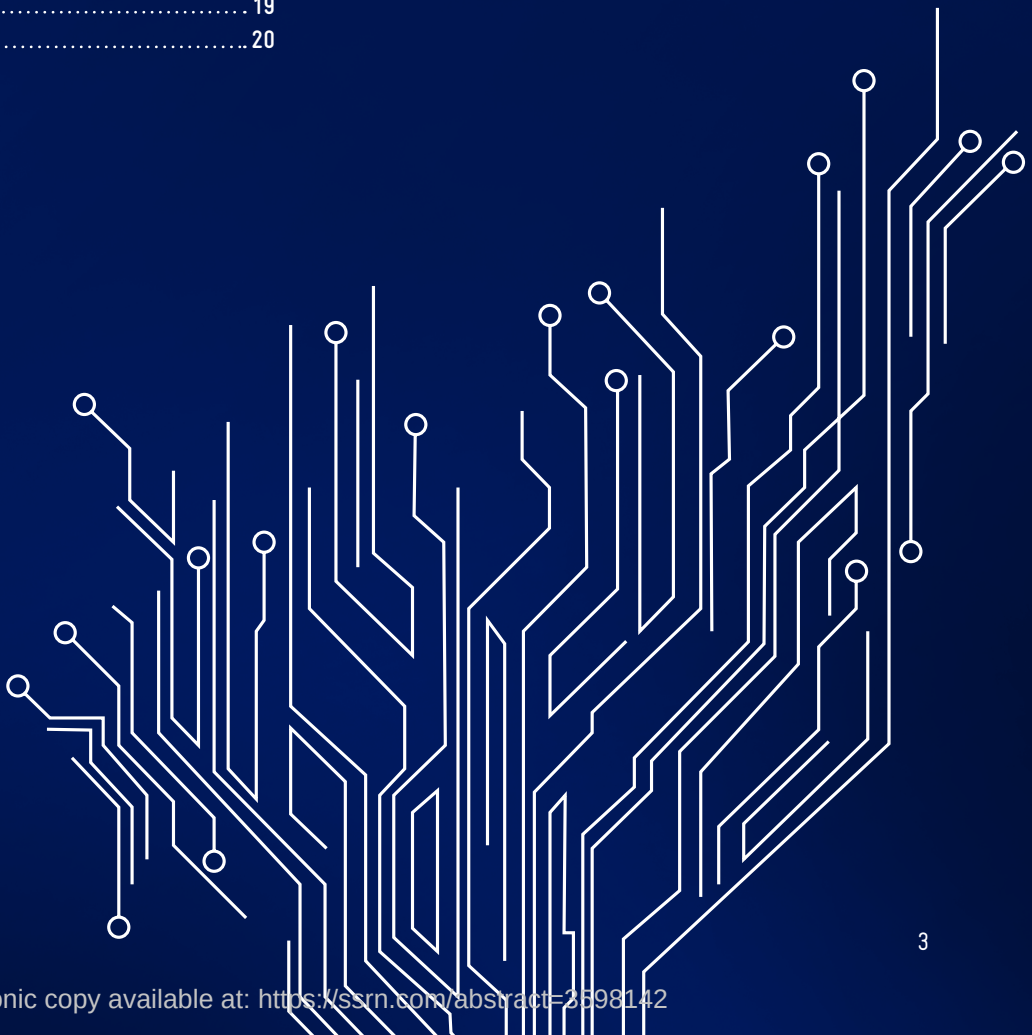
GIZ would like to thank the regulatory and supervisory authorities from Arab countries engaged in the process for participating in the interviews and surveys.

Design:
sweetwater visuelle kommunikation, Darmstadt

Photo credits:
Adobe Stock, Paul Hageman/GIZ

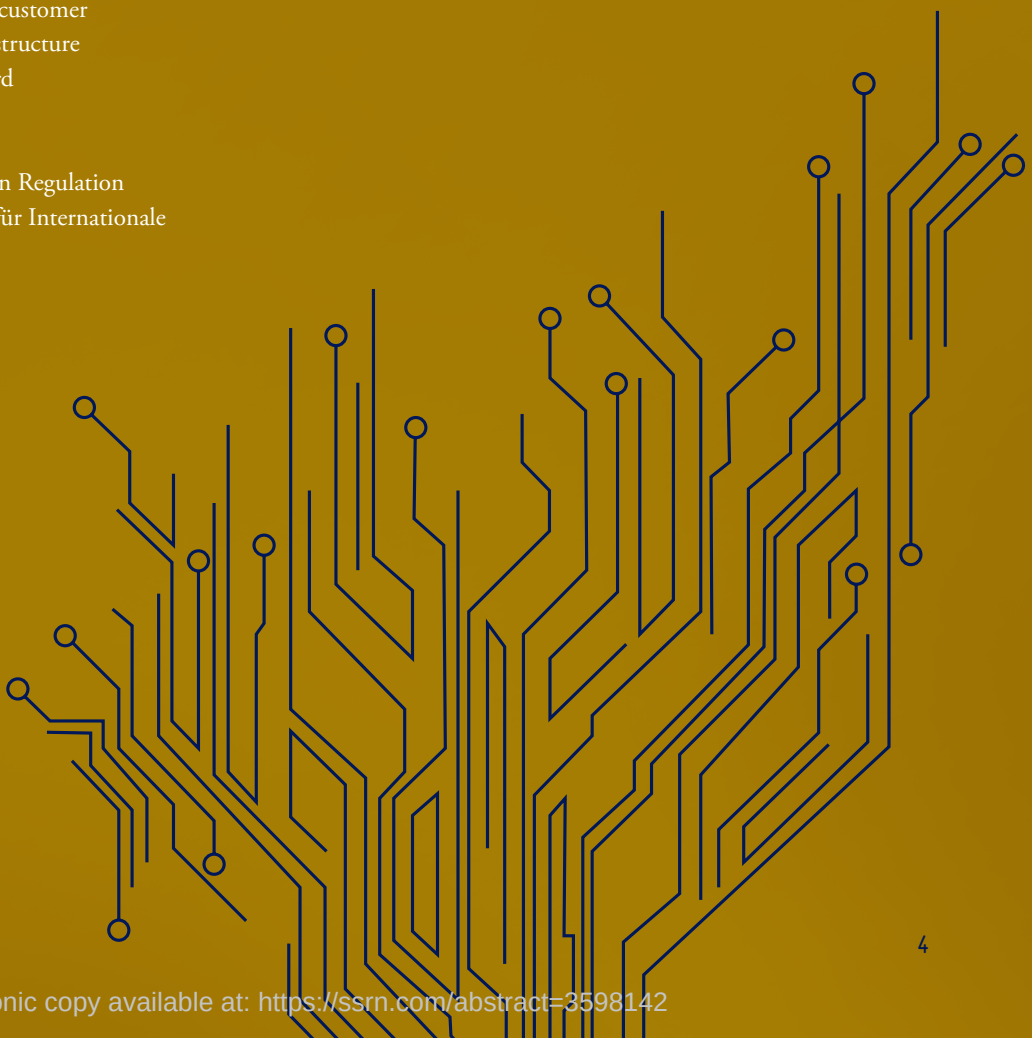
Frankfurt, April 1, 2020.

Contents



List of Abbreviations

ABCD	Artificial Intelligence, Big Data, Cloud Services, Distributed Ledger Technology / Blockchain
AFI	Alliance for Financial Inclusion
AI	Artificial Intelligence
AML	Anti-Money Laundering
ASIC	Australian Securities and Investments Commission
B2B	Business-to-business
B2C	Business-to-consumer
B2G	Business-to-Government
BIS	Bank for International Settlement
CAGR	Compound Annual Growth Rate
CCP	Central Counterparty
CDD	Customer Due Diligence
CERT	Computer Emergency Response Team
CFT	Combating the Financing of Terrorism
CGAP	Consultative Group to Assist the Poor
CLASSIC	Customer-centric, Legacy-free, Asset-light, Scalable, Simple, Innovative, Compliance-light
CTRO	Chief Technology Risk Officer
DLT	Distributed Ledger Technology
DNA	Data, Network Externalities, Adjacent Financial Services
eKYC	Electronic Know-your-customer
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
G20	Group of Twenty
G2P	Government-to-person
GDPR	General Data Protection Regulation
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
HKU	University of Hong Kong
ICT	Information and Communication Technology
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IoT	Internet of Things
ISIP	Inclusion, Stability, Integrity, Protection
IT	Information Technology
KYC	Know-your-customer
MAS	Monetary Authority of Singapore
MENA	Middle East and North Africa
MSME	Micro, Small, and Medium-sized Enterprise
NCP	National Contact Point
NFTS	National Fintech Strategy
R&D	Research and Development
SDG	Sustainable Development Goal
SEC	Securities Exchange Commission
STEM	Science, Technology, Engineering, and Mathematics
TBTF	Too-big-to-fail
TCTF	Too-connected-to-fail
UNSW	University of New South Wales



Executive Summary

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.

1 INTRODUCTION

Finance has been transformed by digitization and datafication over the past five decades. The progress and global reach of technology – particularly information and communication technology – is re-shaping financial services at an unprecedented pace, with incumbents being subject to pressure to change or being disrupted by new entrants or financial institutions that can innovate faster.

Technology-driven financial innovation (Fintech) is grounded in the use of Artificial Intelligence (AI), Big Data, Cloud Services, and Distributed Ledger Technology and Blockchain (ABCD for short). Fintech enables business model, channel and product innovations in finance, and transforms risks.

Finance is the most globalized segment of the world economy and among its most digitalized and data-heavy sectors. This can be seen across four major axes: the emergence of global wholesale markets, an explosion in the number of Fintech start-ups since 2008, fast-paced digital financial transformation in emerging markets and developing economies (e.g. China), and the increasing role of big technology companies (Bigtech) and technology firms (Techfin) in financial services as well as an enhanced interconnectivity of systems.

Digital financial transformation brings about structural changes, with positive and negative effects. While finance and technology have always interacted, the recent speed of change is unique and arises from the co-evolution of financial services, ABCD technologies, internet of things (IoT) and new entrants since the 2008 Global Financial Crisis.

While offering enormous potential, Fintech innovation challenges regulators asked to balance financial inclusion, financial stability, market integrity and consumer protection (commonly referred to as the ISIP framework).

Innovative regulatory frameworks are needed to meet these challenges: regulations that ensure openness to business model, channel and product innovation while addressing risks to society, the financial system, and the economy; and allow experimentation and formal pathways for the entry of Fintech start-ups and other new competitors. This includes proportional (or tiered) regulations for the benefit of a wider range of low-risk, low-cost and low-value financial services.

Regulation is a perennial challenge. Regulatory reform,[1] in times of rapid change, is not evidence of mistake or failure, but quite the opposite, of an active hunt for the best compromise given the (at times strongly diverging) local preconditions. This means the design and degree of regulatory reform will vary among jurisdictions. This toolkit thus serves as a baseline starting point for thorough discussion, rather than presenting ready-made solutions.

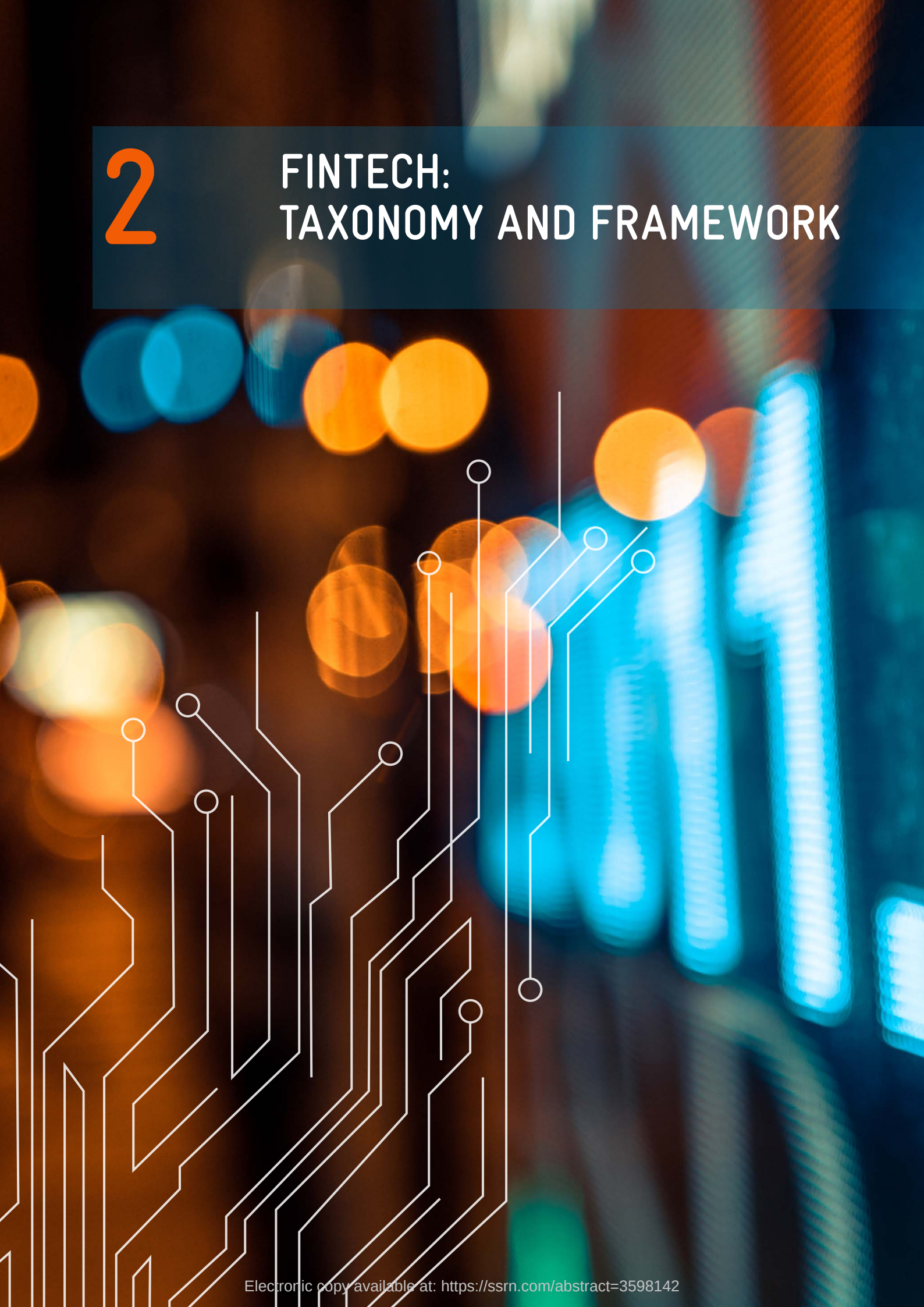
Building on desk research and stakeholder interviews, this toolkit presents regulatory and other approaches to enabling safe Fintech innovation. This report seeks to inform the debate around emerging issues and to support financial policymakers and regulators as well as development practitioners in identifying, formulating, and implementing policy responses, with a focus on the high potential markets of the Middle East and North Africa (MENA) region. The toolkit can be used a) to support the development of an entirely new regularly framework for specific innovations (e.g. in markets with little experience); or b) to enhance existing frameworks to address a range of financial policy objectives in the context of digital financial transformation.

Part 2 presents the taxonomy and framework, Part 3 sets the context and policy objectives of smart regulatory and market approaches to Fintech, and Part 4 introduces the common Fintech challenges and risks against regulatory objectives. Part 5 lays out the foundations for reform, and Part 6 discusses the regulatory tools available for furthering innovation. Part 7 concludes.

Common Definitions of Fintech:

- **Financial Stability Board (FSB):** "technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services."
- **Investopedia:** "new tech that seeks to improve and automate the delivery and use of financial services. At its core, fintech is utilized to help companies, business owners and consumers better manage their financial operations, processes, and lives by utilizing specialized software and algorithms that are used on computers and, increasingly, smartphones."
- **EY:** "Fintechs [are] high-growth organisations combining innovative business models and technology to enable, enhance and disrupt FS. This definition is not restricted to start-ups or new entrants, but includes scale-ups, maturing companies and even non-FS companies, such as telecommunication providers and e-retailers ..."

1 In this toolkit, we use 'regulatory reform' to denote all changes necessary to existing formal laws and regulatory instruments and such new laws and instruments needed to establish an appropriate holistic regulatory framework to respond to innovation.



2 FINTECH: TAXONOMY AND FRAMEWORK

2.1 ABCD Technology Archetypes

2.1.1 Artificial Intelligence and Machine Learning

AI is a very broad umbrella term which refers to systems that perceive their environment and act to maximize their chances of successfully achieving their task. Base line AI is software that mimics human cognitive functions, such as 'learning' and 'problem solving.'

Machine learning is a subset of AI that uses statistical, data-based methods to progressively improve performance on a given task, without humans reprogramming the system to achieve enhanced performance. In practice, learning is achieved through extensive 'practice' with multiple feedback rounds through which the machine is told whether it has passed or failed a task.

AI and machine learning have the potential to develop independently after initial design and creation. It is not necessarily intelligent in the human sense, since it is mostly routine applied repeatedly to generate and structure knowledge regarding the order and correlation of datapoints in a given, potentially very big, dataset. In this sense, AI puts the mass of data gathered by Big Data applications to good use. Such 'narrow' forms of AI have the potential to develop into 'general' forms of AI, potentially exceeding human capabilities in the not distant future.

Prominent use cases of AI and machine learning in financial services include:

- Crowdfunding, including crowd-lending and crowd-investing (where AI assists in allocating liquidity and identifying new funding opportunities)
- Robo advice / asset and wealth managers (where AI assists in finding new profit opportunities and tailoring advice to customers)
- Risk management systems (where AI assists in revealing hidden risk correlations)
- Compliance systems (where AI assists in detecting fraud patterns).

For supervisors, AI may underpin Regtech solutions, which utilize submitted datasets.

2.1.2 Big Data

Big data is separate from but closely connected to AI. Big data analytics refers to the processing of data sets that are either too large or complex for traditional data processing applications. Big data applications apply advanced data analytics methods such as predictive or behavioural data analysis. Big data analytics can be used to detect unexpected correlations in large data pools, test expected correlations for causation, or determine the probability of events.

Big data analytics has received attention from various policy angles, notably the enhancement of potential biases implicit in the data, and the impact of the analytics on privacy and data protection. With advances in computer vision, speech, analytics, and mobile robotics, we can reasonably expect more and more data to be generated.

2.1.3 Cloud Solutions

Cloud services are available to users on demand over the internet from a provider's servers. Such systems may be distributed or centralized. They often provide data storage and access (e.g. Apple iCloud) to a range of software and other services provided by IT and related companies (e.g. Microsoft, Amazon, Alibaba). The major cloud services providers include Amazon, Microsoft, Alibaba, Apple and IBM. Cloud service providers generally begin with storage, computing and analytics services; and, increasingly, are providing a range of related services. Cloud services are often seen as particularly efficient and secure, yet they raise a range of potential issues discussed in more detail below.

Start-ups today are frequently cloud-natives, meaning that from inception their data storage and processing are provided via cloud systems from major providers. Incumbent financial institutions are increasingly using cloud services. Financial services cloud providers such as Amazon, IBM and Microsoft provide traditional software via cloud services (software as a service) and an increasing range of standardised and bespoke cloud-based compliance and data management services.

Regulators too are increasingly looking at cloud solutions for data storage and management. The SEC-sponsored EDGAR disclosure repository website is hosted by cloud service providers including Amazon. The Monetary Authority of Singapore (MAS) has created its own private cloud.

2.1.4 Distributed Ledger Technology, Blockchain and Smart Contracts

A distributed ledger is 'a database that is consensually shared and synchronised across networks spread across multiple sites … allowing a transaction to have [multiple private or] public "witnesses"'.[2] This sharing results in a sequential database distributed across a network of servers all of which together function as a ledger. Distributed ledgers are best understood by considering traditional ledgers in which a centralized register administered by a single entity, like a bank, contains the relevant data. That arrangement entails several risks. If the hardware housing the register is destroyed, the information content may be lost. Second, disloyal employees of the bank may manipulate the information. Third, manipulations and losses may arise from a cyber-attack. While not every server will be cyberattacked, any server can be manipulated with sufficient computing power and time (even if no other encryption weaknesses are known to the attackers). Distributed ledger technology (DLT) addresses these problems by raising the barrier for manipulation. The technology requires consensus of many data storage points (nodes) rather than the approval of one administrator.

Blockchain: Distributed ledgers can be paired with a blockchain protocol. Blockchain refers to the storage of data in bundles ('blocks') in a strict time-related series which links each block to the previous and subsequent blocks. The chronology of storage is revealed through a time stamp imprinted on each of the blocks. The blockchain renders data corruption even harder, because a successful cyberattack requires corrupting not just one block of data, but multiple data sets (i.e. the whole blockchain after the alteration) as well as the time stamps.

Smart Contracts: Distributed ledgers have provided fertile ground for the application of another innovation that may solve the problem of trust in human interactions. While neither smart, nor contracts, and thus not well named, they are self-executing software protocols that reflect parts of an agreement between two parties. The relevant terms are written directly into lines of code. Smart contracts permit the execution of transactions between disparate, anonymous parties without the need for an external enforcement mechanism (such as a court, an arbitrator, or a central clearing facility). They render transactions traceable, transparent, and irreversible (from a technological, though not necessarily a legal, standpoint).

Although distributed ledgers and blockchains are information storage devices, and smart contracts are information processing tools, the latter can 'run' on distributed ledgers. For this reason, we refer to these three technologies collectively as DLTs.

Prominent use cases of DLT include:
- Cryptocurrencies such as Bitcoin, ETH and Libra
- Recordkeeping systems such as share registries and property registries
- Clearing and settlement systems
- Initial Coin Offerings and other forms of token-based finance
- Shareholder and client identification systems (shared registers, eKYC registers, KYC utilities)

2.2 Fintech Provider Types

Providers of Fintech services include start-ups, Techfins and Bigtech, financial institutions, and authorities.

2.2.1 Start-Ups

Start-ups are early-stage firms, typically characterised by a small number of highly motived employees. Start-ups are often, but not always, funded by venture capital.

The typical Fintech is a start-up that identifies a 'pain point' in financial services (something incumbents do poorly or not at all) and seeks to provide a remedy. The usual goal is either to sell the solution service directly to customers or to sell the service or itself to an incumbent financial services firm.

Common Fintech start-up characteristics are expressed in the CLASSIC framework (see figure below).[3]

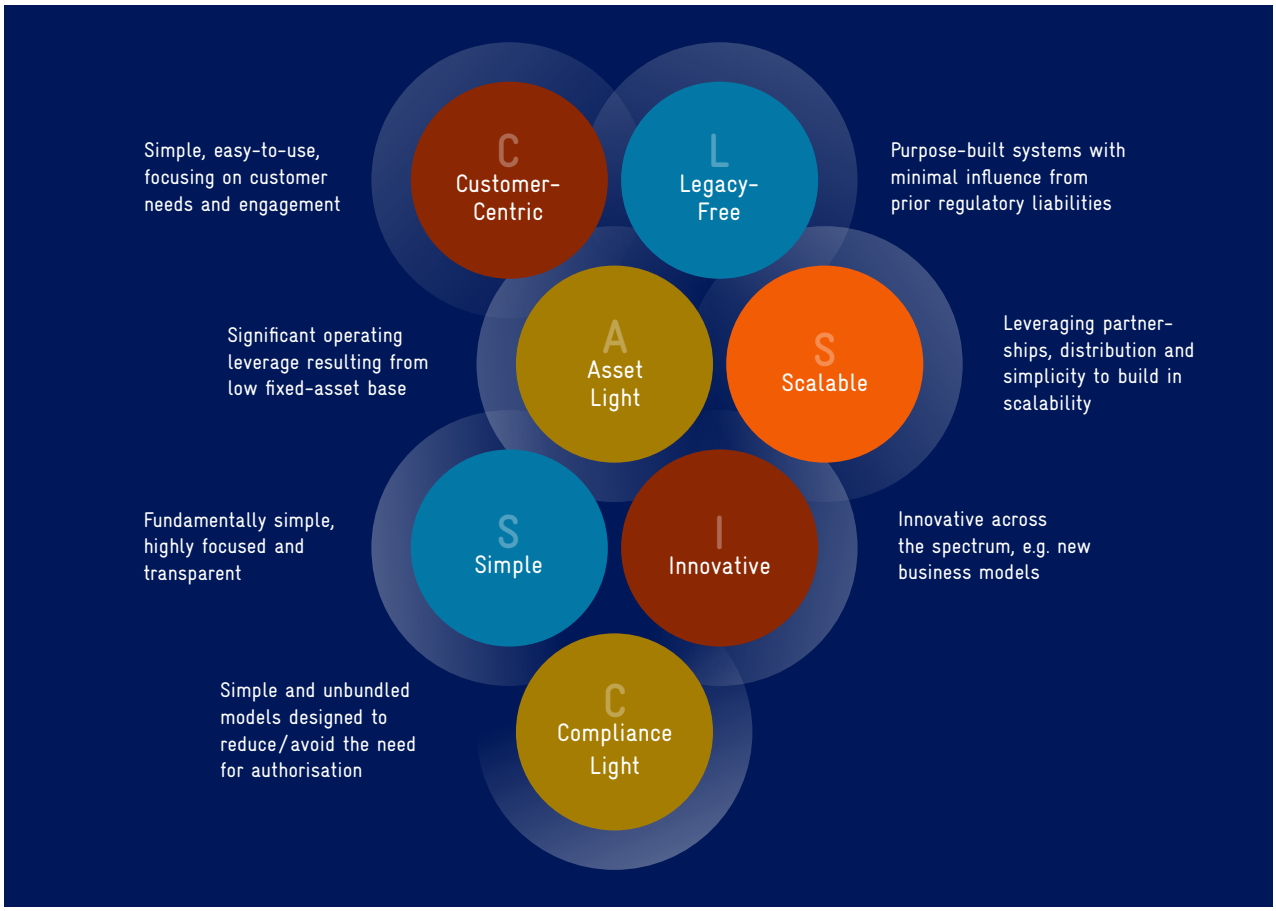
For example, Fintech companies tend to have a laser-like focus on specific customer propositions (often one that is poorly served, if at all, by traditional FS companies) and offer seamless and intuitive user experience. Fintechs are able to scale, typically balance sheet light, and free from the burdens of legacy systems and platforms. Fintechs also tend to have smart, unbundled business models often designed to avoid the need for authorisation.[4]

2 World Economic Forum, Innovation-Driven Cyber-Risk to Customer Data in Financial Services (White Paper, 2017) 6 ‹http://www3.weforum.org/docs/WEF_Cyber_Risk_to_Customer_Data.pdf›.

3 David Lee and Ernie Teo, 'Emergence of Fintech and the Lasic Principles' (2015) 3(3) The Journal of Financial Perspectives: FinTech 1-26 ‹https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2668049›.

4 EY, UK Fintech: On the Cutting Edge (Report, 2016) 21 ‹https://fintechauscensus.ey.com/2018/Documents/EY-UK-FinTech-On-the-cutting-edge.pdf›.

Figure 1 – Characteristics of Fintechs – the CLASSIC Model[5]



2.2.2 Bigtech and Techfin

Bigtechs are existing technology and e-commerce companies (including Alibaba, Amazon, Google, Facebook, Tencent, Apple, etc). These companies often play an important role as cloud service and/or technology service providers to incumbent banks.

Techfins are Bigtechs that enter the financial services market utilising their typically large pre-existing non-financial services customer bases. In contrast to Fintechs, Techfins start with technology and data and then add financial services. Techfins' primary relationships with customers are in other fields such as e-commerce, social networks, entertainment, and telecommunications. They collect massive amounts of data from those relationships, and then seek to use that data to deliver more efficient financial services to their existing customers. Initially, a Techfin may sell data to financial services providers or leverage its customer relationships by serving as a conduit through which its customers can access financial services provided by a separate institution. Later, the Techfin may provide the financial services directly itself. Techfins can assemble much of the information the customer's bank or asset manager possesses, and supplement it with very detailed knowledge of many other aspects of customer choices and preferences. These preferences can then be processed by algorithms that have established correlations between certain preferences and creditworthiness to provide a much more nuanced assessment of creditworthiness than a bank.

The BIS summarizes these key characteristics of Bigtechs evolving into Techfins under the acronym DNA: data, network externalities, adjacent financial services.[6]

Techfins pose major regulatory challenges for competition, data privacy and cyber security. From a regulatory perspective, they need to be approached differently than Fintechs. The provider with the best information about a customer is best placed to price credit and insurance services for that customer. Traditionally that has been the customer's bank. However, banks may no longer enjoy this advantage or at least not for long.

5 Diagram adapted from EY (n 4) 22.

6 BIS, Annual Economic Report 2019 (Report, 2019) 62 ‹https://www.bis.org/publ/arpdf/ar2019e.htm›.

The data to which Techfins have access is typically expansive, covers much of the people in a market, and deep in terms of the number of data points that can be gathered for an individual. Techfins can readily expand into offering financial services. Facebook, Amazon and Alibaba are doing so in payments in India — a competition which is likely to be played out in an increasing range of markets around the world as Alibaba has shown with its expansion of financial services offerings in China, particularly in lending and investment management.

2.2.3 Financial Institutions

Financial institutions can use Fintech from the ground up sparing legacy systems and legacy processes, such as digital (or challenger) banks, that harness digital technology to provide more client-oriented, convenient and cheaper branchless banking services. Alternatively, traditional commercial banks leverage the latest wave of technology such as big data analytics in risk management or, in other cases, non-bank financial institutions digitally transform their operations and client relationships.

2.2.4 Authorities: Regtech / Suptech

Regtech is the use of technologies for compliance and reporting as well as regulation and monitoring. It thus includes Suptech as one component. Regtech systems are used to enhance operations (Operations Regtech)[7] and compliance controls within the providers (Compliancetech) as well as supervision (Suptech) processes.

Regtech is thus an umbrella that covers private sector applications in which regulatory compliance, monitoring, and analytics are digitalized and automated for efficiency gains. From the regulatory and supervisory standpoint, it includes use of technology to facilitate oversight by financial supervisors mostly using big data analytics and, increasingly, AI.[8] Regtech tends to enable more efficient compliance with regulation and Suptech more efficient supervision.

Regtech includes electronic know-your-customer (eKYC) systems which facilitate client on-boarding by financial intermediaries and can enhance market integrity, automated compliance monitoring and reporting. Regtech also brings new challenges, including the need for qualified supervisory staff, adaptations in internal governance and new cybersecurity risks.

2.3 Fintech Markets

2.3.1 G2P – Government-to-Person

Fintech markets emerge among a range of parties including government, businesses and retail clients. Government-to-private markets include, for example, official identity schemes, such as Aadhar in India or the European eIDASR, the scheme for cross-border digital identity, and electronic systems for payment of government salaries and benefits.

2.3.2 B2B – Business-to-Business

B2B markets include, for example,

- data service providers such as *Refinitiv, Thompson-Reuters and Bloomberg*
- AI-driven risk analytics, including *Blackrock's Aladdin*
- business-oriented mobile payment services
- most blockchain-as-a-service offerings, for instance by *IBM* and *Microsoft*
- enterprise cloud services

2.3.3 B2C – Business-to-Consumer

B2C markets include, for example, remittance services for migrants, mobile payment services for consumers, and robo-advice and wealth technology solutions.

2.3.4 B2G – Business-to-Government

B2G markets include, for example, cloud storage for government entities, outsourced development of risk analytics and supervision tools, and electronic payment systems (e.g. public-private real time gross settlement (RTGS) systems.

7 Luca Enriques and Dirk A Zetzsche, 'Corporate Technologies and the Tech Nirvana Fallacy' (Law Working Paper No 457/2019, European Corporate Governance Institute, 25 June 2019) 4 https://ssrn.com/abstract=3392321; Douglas Arner, Janos Barberis and Ross Buckley, "FinTech, RegTech and the Reconceptualization of Financial Regulation" 37 Northwestern Journal of International Law and Business 371, 371–414 (2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847806.

8 Janos Barberis, Douglas Arner and Ross Buckley (eds), The RegTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation (J. Wiley 2019).

3 CONTEXT AND POLICY OBJECTIVES OF SMART REGULATORY AND MARKET APPROACHES TO FINTECH

3.1 Fundamental Trends in Fintech and Financial Regulation

Fintech is transforming financial systems and challenging existing approaches of financial policymakers and regulators. Overall, four fundamental trends can be observed.

3.1.1 The Type of Players in Financial Services Are Changing

This change calls for regulatory and supervisory responses to safeguard financial integrity, protection, and stability. As start-ups, Bigtechs and/or Techfins enter markets, regulators need to be nimble and adaptive. Start-ups and Techfins benefit from different unit economics: start-ups from asset-light, less regulated, partly outsourced business models, and Techfins from economies of scale (platforms) and network effects. The range of business model, channel, and product innovations typically challenges regulators in terms of regulatory scope, frameworks, skillsets and approaches.

3.1.2 Traditionally Segregated Sectors Are Converging

This change triggers more inter-institutional coordination among regulators and requires more regulatory resources at least in the short-term. Policymaking and regulation for Fintech needs to be coordinated across jurisdictions, including prudential and non-prudential financial supervision, competition policy, ICT, and cybersecurity.

3.1.3 The Rate of Innovation and the Amounts of Data Are Changing

This change requires more active regulators. Fintech innovations are emerging ever faster, increasing the volume, velocity, and variety of data. Risks often increase alongside increasing reliance on technology, interconnectedness in the financial system, and concentration of data. The rise of data can challenge market competition (e.g. platform economies) and cybersecurity (e.g. open data and outsourcing), among other factors. So, an abundance of data tends to challenge regulatory resources. Regulators need to respond with their own Regtech and Suptech data-driven tools.

3.1.4 The Objectives for Regulators and Their Tools Are Changing

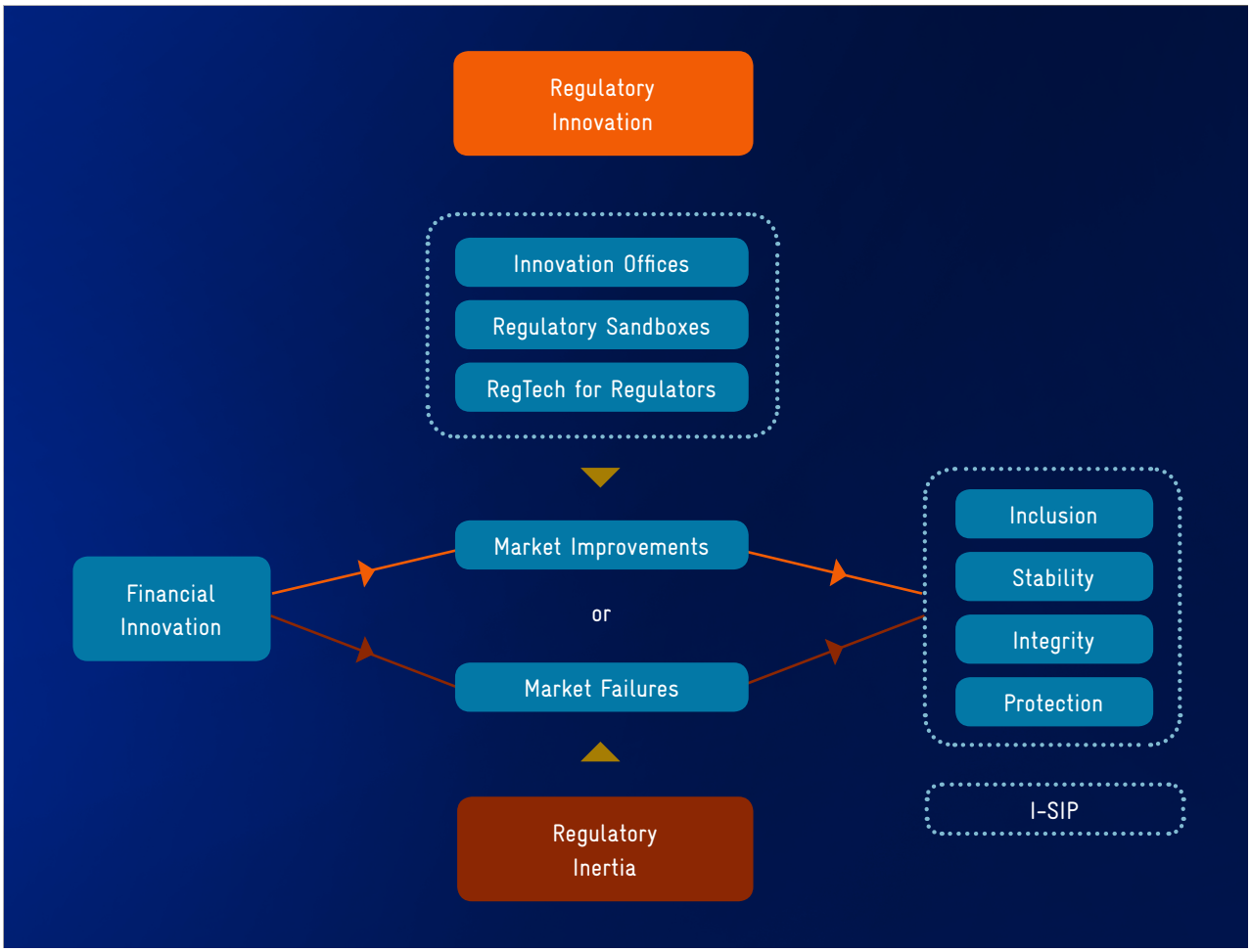
Many financial systems are insufficiently competitive and do a poor job of serving certain market segments, especially small business and consumers. Policymakers consequently often welcome Fintech and task their regulators with its encouragement to promote competition. This calls for new approaches by regulators which may include more frequent consultation with providers, innovation hubs, regulatory sandboxes and Regtech, as they seek to fulfil a market facilitator role.

3.2 Overarching Policy Objectives: The ISIP Framework

Fintech innovation[9] has the potential to stimulate competition and product variety in terms of quantity (financial sector broadening) and quality (financial sector deepening and market efficiency). Financial regulation is required to ensure this innovative technological progress has positive outcomes for the society and economy. Regulatory approaches need to ensure that Fintech innovation contributes to overarching financial policy objectives such as inclusion, stability and integrity of the system, and client protection (ISIP).

9 Some differ between different types of innovation such as adjacent, disruptive, or breakthrough innovation. The boundaries of these expression are hard to define. From our perspective all innovation shares the joint feature to drive efficiencies, either by assisting incumbents to perform services better or less expensively (collaborative approach) or by replacing incumbents altogether (disruptive approach).

Figure 2: A Framework of Fintech Innovation and Financial Policy Objectives[10]



- **Financial inclusion:** all people and firms have access to, and are able to use, affordable, responsible and sustainable financial services.
- **Financial stability:** a multidimensional concept, of which one aspect is a robust and smooth functioning financial system.[11]
- **Market integrity:** illicit financial transaction and market participants in the financial system are controlled with AML/CTF risks as prime examples.
- **Client protection:** clients' funds are protected from non-compensated financial and operational risks such as moral hazard, fraud, deficient operations, and data protection.
- Some frameworks mention competition as a separate policy objective – a goal which typically requires regulators to rethink their role.

10 Figure reproduced from UNSGSA FinTech Working Group and CCAF, Early Lessons on Regulatory Innovations to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes, and RegTech (Report, 2019) 16.

11 See Serge Jeanneau, Financial Stability Objectives and Arrangements – What's New? (BIS Papers No 76) <https://www.bis.org/publ/bppdf/bispap76e_rh.pdf>.

3.3 Fintech Disrupting the Financial Systems in the MENA Region

By global standards, financial sectors in the MENA region are moderately developed in terms of depth and market composition. They are dominated by banks with non-bank financial services emerging. The countries of the Gulf region have larger and deeper financial systems than the more diverse group of non-Gulf countries. Hence, oversight in these bank-dominated markets is pre-dominantly characterised by a traditional focus on prudential supervision led by institutional regulations.

All together the financial inclusion levels in the MENA is 63 % of adults.[12] Micro, small and medium-sized enterprises (MSME), particularly informal ones, make up the largest share of the private sector but are severely constrained due to generally low bank competition paired with regulatory gaps for alternative financial services and a fairly stagnant financial infrastructure (including digital or faster payments, effective credit bureaus, collateral and movable asset registries). The informality and limited capacities of these businesses impede financing by incumbents given their attitudes to risk and the relatively high costs of servicing such businesses.

Fintech offers to spur competition and promote financial inclusion (or deepening) and economic development. The use of Fintech in identification and KYC procedures, payments and money transfers, lending, investments and savings, insurance, and public administration as well as in supervisory and regulatory practices offers a great deal to the MENA region.[13]

ICT, financial services, and their convergence in Fintech are widely considered growth sectors and enablers of new jobs and structural diversification in these countries on their path to digital economies: e.g. in Egypt every new ICT job created 2.8 indirect jobs between 2008 and 2011; and M-pesa in Kenya directly generates income for more than 80,000 agents in addition to the effects of increased levels of financial inclusion.[14]

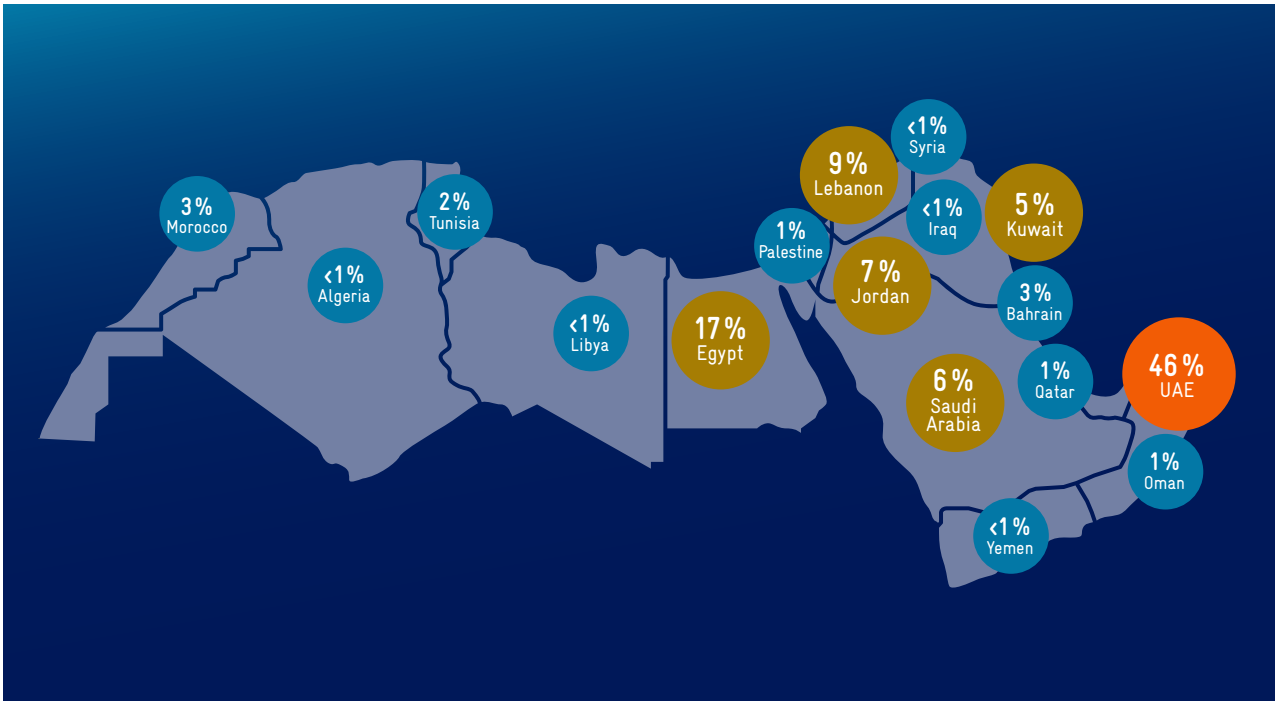
© Paul Hageman / GIZ

12 Asli Demirgüc-Kunt et al, The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution (The World Bank Report, 2018).

13 Douglas W Arner, Ross P Buckley and Dirk A Zetzsche, Fintech for Financial Inclusion: A Framework for Digital Financial Transformation (AFI Report, September 2018) ‹https://www.afi-global.org/sites/default/files/publications/2018-09/AFI_FinTech_Special%20Report_AW_digital.pdf›; Douglas W Arner, Jànos Barberis and Ross P Buckley, 'Fintech, RegTech and the Reconceptualization of Financial Regulation' (2017) 37(3) Northwestern Journal of International Law and Business 371; Dirk A Zetzsche et al, 'Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation' (2017) 23 Fordham Journal of Corporate and Financial Law 31; Douglas W Arner et al, 'Fintech and RegTech: Enabling Innovation While Preserving Stability' (2017) 18(3) Georgetown Journal of International Affairs 47; Dirk A Zetzsche et al, 'From Fintech to TechFin: The Regulatory Challenge of Data-Driven Finance' (2018) 14(2) NYU Journal of Law and Business 393.

14 World Bank, Iraq Systematic Country Diagnostic (Report, February 2017) ‹https://elibrary.worldbank.org/doi/abs/10.1596/26237›; World Bank, A New Economy for the Middle East and North Africa (MENA Economic Monitor Report, October 2018) ‹https://openknowledge.worldbank.org/bitstream/handle/10986/30436/9781464813672.pdf?sequence=11&isAllowed=y›.

Figure 3: Distribution of Fintech Start-Ups Across MENA Countries, 2018[15]



Fintech in the MENA region is driven by an increasingly well-educated and tech-savvy young population and by the scale of opportunity. Record remittance flows that move on legacy rails, the numbers of unbanked people and the massive funding gap for millions of businesses across the region incentivise Fintech start-ups, Bigtech or Techfins, and innovative financial institutions to harness the possibilities of Fintech. The number of Fintech start-ups has grown rapidly over the past years, at a CAGR of 39 % since 2012, with more than 300 Fintech start-ups present across the MENA region (see figure).[16]

15 Magnitt, 2019 MENA FinTech Venture Report (Report, October 2019) ‹https://magnitt.com/research/50675/2019-mena-fintech-venture-report›.

16 Wamda, Fintech in MENA: Unbundling the Financial Services Industry (Report, 16 March 2017) ‹http://backend.wamda.com/api/v1/downloads/publications/fintech-mena-unbundling-financial-services-industry›; Magnitt (n 16).

4 COMMON REGULATORY CHALLENGES AND RISKS WITH FINTECH

4.1 Inclusion

4.1.1 Fintech-Related Inclusion Issues

Remarkably, since 2010, over 1.2 billion people globally have opened their first ever financial or mobile money account. Yet a lot still needs to be done, with 1.7 billion adults lacking formal access to a financial or mobile money account as of 2018, and in turn to other types of financial services. One must furthermore look beyond technical inclusion: such an account is a precondition to participation in the financial system, not an end in itself. Such participation is about improving people's lives and supporting sustainable development in the context of the UN Sustainable Development Goals (SDGs). The account is a means to an end which will be enabled by more efficient everyday living, investments in education, health and retirement, and greater resilience against economic shocks. Account holders who lack the knowledge to use financial services effectively can face new types of financial difficulties, such as over-indebtedness or insolvency. A broad concept of financial inclusion is thus necessary: in addition to formal access, true financial inclusion requires financial and technological literacy, technological infrastructure, trust in financial firms and regulators, competitive choice, etc.

Fintech-driven products and services, if appropriate, accessible and affordable, can do much to promote financial inclusion.

4.1.2 Inclusion-Related Policy Tools

Realizing the potential of Fintech for financial inclusion calls for a strategic framework for an enabling environment of policies, regulations, and infrastructure. The Alliance for Financial Inclusion (AFI) draws from experience in EMDEs and suggests a progressive approach in four staged phases to building a Fintech ecosystem for financial inclusion:[17]

- Digital identification and simplified account opening
- Open access interoperable electronic payment systems
- Government provision of services including salary and benefit payments through the ID, account and payment infrastructure
- Development of digital financial infrastructure such as clearing and settlement systems.

These pillars work best in a well-designed proportional regulatory system that supports financial inclusion, other financial policy objectives (stability, market integrity, consumer protection) and sustainable development aligned with the SDGs.

4.2 Stability

The global financial crisis of 2008 ushered in a new era in financial stability regulation. Before 2008 our system focussed on the stability of individual financial firms. The crisis shone a spotlight on the potential of linkages among firms to be a source of systemic risk and so post-crisis regulation has focussed far more on interdependencies in markets.

We address the full range of Fintech-related financial stability issues in Annex I. These issues include cybersecurity, market structure, data protection, and financial infrastructure (particularly, the rapidly growing role of cloud services).

We then consider in the Annex seven stability-related policy tools available to regulators to respond to the risks associated with the instability inducing aspects that may arise from the growth of Fintech. The first of such responses is to prioritise tech risk. Tech risk is a new form of risk, and thus not yet prominent in most financial regulators thinking – and it needs to be. The next steps for regulators are to strengthen their in-house tech expertise and enhance reporting requirements about firms' tech risk management strategies. Further strategies are also considered. We then conclude by analysing why regulators themselves need to start employing Regtech solutions in supervision.

4.3 Integrity

4.3.1 Fintech-Related Integrity Issues

Financial market integrity focuses on preventing the criminal and terrorist use of the financial system, with fraud and theft the most common examples. These activities undermine social acceptance and trust in financial services. Illegal conduct can

17 Arner, Buckley and Zetzsche, Fintech for Financial Inclusion: A Framework for Digital Financial Transformation (n 13).

be profitable to financial firms. For instance, firms that support money laundering and tax evasion may well charge unusually high fees. This increases risks for society, and for legitimate clients of such firms.

Much financial regulation and financially related law enforcement activities relate to the intersection between criminal activities – especially fraud and theft – and the use of the financial system to support criminal or other prohibited activities such as terrorism. Fintech offers a range of new tools to potentially combat such activities (frequently in the form of Regtech). However, Fintech can also offer new scope and means for such criminal activity.

From the standpoint of criminal activity relating to finance, digital crime is the most rapidly growing area of crime in recent years, as a range of crimes (such as fraud) move into the digital environment. High profile examples include digital frauds, cyber thefts and identity and data thefts. Technology has enabled much wider access through social media and into bank accounts and other electronic stores of financial and data resources. In this respect, a focus is the development of cryptocurrencies and other forms of digital assets, that offer new opportunities for fraud and money laundering.

4.3.2 Integrity-Related Policy Tools

Integrity-related policy tools include:

- eKYC and digital due diligence -- given the pro-concentration forces of technology, we expect the former will, in time, lead to a series of eKYC utilities covering whole financial markets,
- Electronic compliance and risk management applications detecting criminal activity (insider trading, fraud, money laundering etc.) by looking for unusual data patterns,
- Automatic tax information exchange among public authorities, and in certain cases private entities,
- Further cooperation among public and private entities to implement and enforce uniform standards across market participants,
- Enforcement action and sanctions.

4.4 Client Protection

4.4.1 Fintech-Related Client Protection Issues

Client protection covers mainly transparency, fair treatment, data privacy and confidentiality, and complaints handling. Issues for clients of Fintech firms may include:

- fraudulent or criminal activity or malfunctions,
- implicit discrimination in big data analytics,
- data privacy infringement, data security issues with the provider or in outsourcing arrangements,
- profiling of clients using multiple layers of data from different sources and providers

4.4.2 Client Protection-Related Policy Tools

Policy tools aiming at client protection include:

- mandatory disclosure of key facts and statements,
- product governance and target market rules,
- mandatory training and licensing of client advisors,
- testing algorithms for undisclosed or unexpected side effects,
- clear data privacy and security legislative frameworks including consent, right to be forgotten, limitation of data storage,
- allocation of liability with a potentially reversed burden of proof for complex algorithms and other non-transparent infrastructure.

5 LAYING THE FOUNDATIONS FOR REFORM

5.1 Principles for Smart Regulatory and Market Approaches

The fundamental changes taking place in the financial system globally and in the MENA region call for the design of adequate regulatory approaches to Fintech innovation. As innovation usually requires an enabling environment, regulatory frameworks will determine the future of Fintech. Basic principles for financial policymaking and regulatory reform in the MENA countries can be borrowed from global good practice and include: 1) activity-based regulation, 2) proportional regulation, 3) globally consistent regulation, 4) regulation that lowers barriers to entry, and 5) technology-neutral regulation.

5.1.1 Activity-Based Regulation

Financial regulation should be based on activities, on the functions, being performed, instead of the type of organisation or firm that performs them. The same activity with the same risk should attract the same regulatory treatment.[18]

Effective regulation of fintech has to consider the nature of the financial risks and of the entities bearing the risks. Understanding who bears the financial risk is instrumental in developing appropriate and effective regulatory tools and the right place to start in developing this understanding is the nature of the activity being performed.

5.1.2 Proportional Regulation

Especially with Fintech, because so many Fintech start-ups are small, regulation needs to be proportional with lighter rules for smaller entities and more rigorous rules for the major institutions.

5.1.3 Global Fundamentals

'Smart' regulation should be built on shared fundamentals. As an example, while all agree on the importance of combatting money laundering and financing of terrorism (AML/CFT) and the Financial Action Task Force sets standards, implementation of these standards varies among countries which is problematic. To resolve this tension, regulators should look to their broader mandates (i.e. consumer protection, financial stability, competition, etc) as opposed to attempting to apply overly rules-based approaches and should seek a high level of consistency with details.

5.1.4 Towards Lower Entry Barriers

Regulators should seek to promote competition in their financial markets, and if promoting competition is not an explicit part of their mandate, they should seek to have it included. Competition and innovation are two sides of the same coin in finance: innovation enables competition, and competition drives innovation as one competitor seeks to distinguish itself from the others. So, competition on the merits (i.e. where all participants follow the same rules and bear the same costs) is in general a good thing in finance. It can be difficult to determine if a new Fintech entrant is a competitor or collaborator. Some Fintechs follow disruptive strategies, while others support licensed entities in mastering the digital revolution. Both approaches are healthy and support the financial ecosystem. On balance, and certainly for all jurisdictions that wish to signal regulatory flexibility to the market, the express provision of the promotion of both competition and innovation in their mandate will be most useful.

New participants can facilitate regulatory experiments with new supervisory and reporting models. The bargaining power of start-ups with regulators is disproportionality low compared to that of large incumbent licensed enterprises. This gives regulators the opportunity to engage in a sequenced reform process and to impose new digital regulation on such new entrants from the outset, while incumbent financial institutions will only have to face more digitised monitoring and reporting over time. This allows experimentation at the margin (as supported by the low numbers of firms in sandboxes) while the bulk of the industry is gradually and more slowly brought to new standards via the digitisation of regulatory requirements themselves, in short: Regtech. Risks incurred by unregulated, yet sandboxed, firms may be accepted — for the very reason that they can kickstart innovation whereas regulation sets higher-than-desired barriers to innovation.

Overall, it is reasonable to develop smart regulatory approaches, i.e. frameworks that lower entry barriers to financial markets in so far as it is still possible to keep risks at the entry gates.

18 Robert C Merton, 'A Functional Perspective of Financial Intermediation' (1995) 24(2) Financial Management 23.

5.1.5 Technology-Neutral Regulation

Regulation should be 'technologically neutral'. This does not excuse regulators from the need to understand the impact of new technologies on processes (e.g. biometric identification for payments) or business models (e.g. alternative data credit scoring). Instead 'technological neutrality' means regulators do not seek to 'regulate' technological innovations, but instead focus on the financial processes and activities that technology enables and that ought to be subject to regulation (e.g. the problem is not automated investment advice but the risks of fraud and poor advice).

5.1.6 Seven Stages of Smart Regulatory Approaches

From this basis, a reasonable regulatory approach comprises sequenced stages:

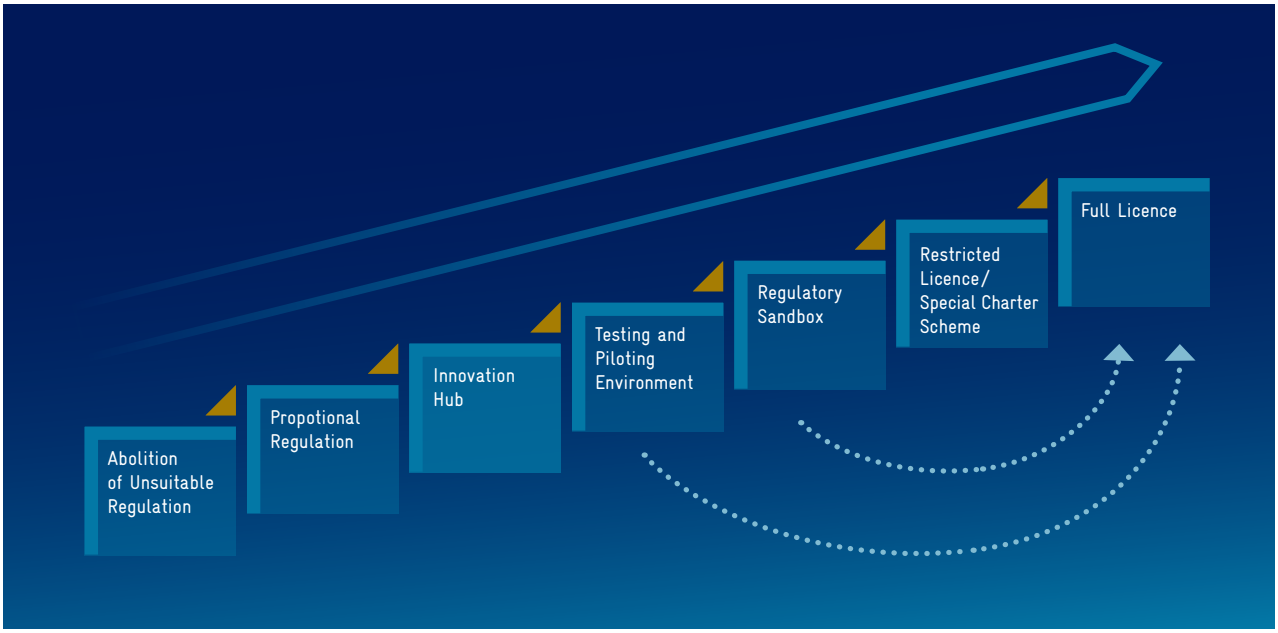
1. **Abolition of unsuitable regulation**
2. **Proportional regulation**
3. **An innovation hub,** which does not require legislation, is staffed by regulatory experts that guide Fintech firms through the regulatory maze, discuss their innovation, and can issue waivers or other forms of dispensation
4. **A testing and piloting environment**
5. **A regulatory sandbox,** which widens the scope of testing and piloting, is transparent, and removes the regulators' disincentive to grant dispensations (and depending on the ecosystem and the importance of cross-border recognition the sandbox may take the form of a sandbox umbrella)
6. **A restricted licensing / special charter scheme,** under which innovative firms can further develop their client base and financial and operational resources
7. **A full licence,** based on a proportional structure, when size and income permits

There are a range of reason for this order of sequencing. First and foremost, regulators must identify and reduce red-tape 'formal' regulation and ensure proportionate regulation, i.e. any regulatory requirement is justified with risks (assumed or proven) relating to the very activity. Once this is ensured, an innovation hub is the most flexible approach and likely to be of most benefit to the widest number of firms. It facilitates contact for Fintech firms with the regulator and will boost regulator learning. Testing and piloting and sandbox regimes in contrast, will assist some firms, but not all, and often, not many. These initiatives are worth having but will not be of broad appeal. Finally, the restricted and full licensing regimes are desirable and essential, of course, respectively, but naturally come towards the end of the product development process.

Furthermore, from one stage to the next, regulatory rigour and fixed costs of regulation increase, as does the Fintech's operational space in terms of clients, resources, and scope. This sequence of regulatory approaches should lead to a desirable lowering of entry barriers for firms.

At each stage, of course, the Smart Regulator will consider risk considerations in the context of the firm's ability to cover costs and while seeking to maintain a similar regulatory burden for licensed entities).

Figure 4 – Seven Stages of Smart Regulatory Approaches



5.2 Principles for Financial Systems Development Cooperation

5.2.1 Technical Assistance and Capacity Development for Fintech Innovation

Donors, development finance institutions, and bi-/multilateral agencies just like GIZ can harness international partnerships, their long-standing bilateral cooperation relationships across the MENA region, and their experience in systemic approaches to financial systems development. Technical (and financial) assistance however will have to respond to the fundamental changes taking place on the market and regulatory levels of the financial system.

Advisory will have to go hand in hand with institutional and human capacity development to address challenges in IT and financial innovation including, but not limited to:

- the technical and vocational education, training, and recruitment of technology and financial young potentials and creation of attractive career paths in the sector;
- the promotion of institutional IT expertise as well as policies and procedures within regulatory and supervisory authorities as well as providers across functions and hierarchy levels;
- the development of capacities of staff can help to drive forward technology and innovation-related topics within the regulatory and supervisory authorities;
- the exposure of senior decision makers and young potentials to one another within organisations as well as across authorities and financial service providers.

Financial systems development initiatives, such as for digital financial inclusion, might require more than ever a cross-country, cross-sectoral, and multi-level approach. On the national level, this may entail:

- Re-visiting and re-defining stakeholder maps for any one financial system initiative so as to consider all relevant players from within the wider ecosystem, such as associations and providers from ICT sectors or authorities relevant for competition, cybersecurity, digital economy or e-government and the like;
- Establishing a dedicated unit within the Central Bank staffed with Innovation Officers in charge for Fintech and regulation-related external inquiries, in-house advisory, market monitoring, and facilitation of below mentioned measures (Innovation Hub);
- Organising Hackathons whereby competent authorities challenge teams of technology experts (Regtech), Fintech start-ups or other service providers to develop and pitch their solutions for a given problem statement against some monetary incentive;
- Organising Tech Fairs whereby public and private stakeholders invite for, exhibit and review latest technology and innovation developments;
- Organising Open Days whereby authorities invite young entrepreneurs and tech firms to inclusive visit for an open dialogue;
- Supporting co-working spaces, incubators or Digital Centres (see BMZ initiative) and the like in public-private-civil society partnerships;
- Organising a Fintech Council for regular public-private dialogue, the exchange of knowledge and consultations between policymakers, regulators, practitioners, and academia, or for joint policy or other working papers;
- Setting-up a governance framework and coordination structure with the Central Bank as lead organisation and thematic working groups with public-private players in an effort to formulate and implement national policies and strategies (e.g. national Fintech strategy), infrastructure projects (e.g. CERTs, data infrastructure, KYC utilities, payment gateways etc) and industry standards (e.g. open data and API platforms);
- Interdisciplinary training of staff of authorities in innovation, business, technology, strategy development, project management, and marketing matters;
- Enhancing national digital and financial literacy levels in collaboration with public, private, and civil society stakeholders.[19]

On a **regional level**, partner countries could join forces for:

- Providing a safe environment for regional cooperation and experimentation in innovation topics for financial regulators to strengthen their capacities and a regionally integrated framework for Fintech. Interested authorities engage in learning, supervisory exchange, joint testing, and co-licensing in Fintech and Regtech issues. They jointly work towards a regime for regulatory passporting to enable the regional expansion and growth of Fintech;
- Setting up regional Centres of Expertise in specific areas, with access to expertise and trainings in a fair and equal manner for all participating countries and stakeholders (e.g. Regional Cybersecurity Resource Centre).

19 See 'Systemic Approach to Financial Inclusion', CGAP (Web Page) <https://www.cgap.org/topics/collections/market-systems-approach>.

5.2.2 Ecosystem Stakeholder Engagement and Consultation

A consultative reform process is critically important to strengthening the entire ecosystem for Fintech, including governance, demand, talent, capital-related enablers, and especially for developing an enabling regulatory framework. Implementing regulatory reform is a complex undertaking and requires the interaction of a broad array of stakeholders. The regulatory framework should aim to balance the interests of relevant stakeholders in order to achieve the desired impact for the sector, the society, and the economy.

© Paul Hageman / GIZ

5.2.3 Holistic, Active, Coordinated In-Country Policymaking

Ensuring a clear, long-term perspective for Fintech reform and investments is crucial for attracting and ensuring the needed contributions. That long-term perspective will require policymakers and regulators, infrastructure and market players to convene under a common theme and strategy. This requires strong leadership, hence the advice to appoint a lead agency such as the Central Bank or, if desired, as high as the Prime Minister's or President's Office.

Once the Fintech reform agenda is started, interventions may have to be adjusted. However, corrections should be limited to the original strategy framework. A reshuffling of priorities along the way, depending for example on political events such as elections, are likely to create confusion and deter investments.

There are no silver bullets and no one-size fits all solutions. Knowledge of the local context paired with good practice and lessons learned from other country experiences promises sustainable results. Regulatory reforms must fit the enabling environment (political, economic, social, technological, legal) of any one country and focus on achieving local optima. For example, conventional financial solutions may face difficulty with some parts of the society and hence Islamic financial principles such as risk-sharing or profit-and-loss-sharing may be relevant.

Self-confidence in learning and home-grown solutions are key. This includes preparing institutions for the reality that Fintech reform can be an ongoing, multi-year process, rather than a one-step effort that yields short-term results.

6 RECOMMENDATIONS FOR THE DESIGN AND IMPLEMENTATION OF SMART REGULATORY AND MARKET APPROACHES TO FINTECH INNOVATION

Fintech is a means to achieve ends. The ends relate to specific policy objectives. Fintech policymaking in the MENA region should, as it does in most places, seek to use innovative regulatory approaches to promote Fintech in the pursuit of greater competition in financial services and financial inclusion. Further regulatory adaptations will be needed so that the growth in Fintech does not compromise the three traditional financial regulatory aims of promoting financial stability, integrity, and consumer protection.

This chapter outlines general preconditions for reform and presents innovative regulatory and market approaches which are appropriate for MENA countries and through which financial policymakers and regulators can promote innovative Fintech businesses and the ISIP framework.

6.1 Preconditions

6.1.1 Diagnostic Studies

Diagnostic studies involve environmental assessments and market analyses to help identify the key drivers of, and challenges to, the growth of Fintech in a country. The studies seek to understand the status quo, and thereby underpin recommendations for reform. The environmental assessment typically encompasses the political, economic, social, technological, legal, capital, and human resources aspects of the Fintech ecosystem. The market analysis will address supply and demand for Fintech so as to support evidence-based policymaking and private sector investments. The data collected should help to challenge assumptions, support new policy approaches, and provide the basis for monitoring progress.

6.1.2 Definition of Fintech

Fintech is a broad term often used flexibly. A clear definition of Fintech is thus key to developing adequate regulatory frameworks.[20] The definition does not necessarily need to be codified in law. A softer definition might be helpful as it allows flexibility for adjustments over time. Generic definitions, as listed in the introductory part, can serve as examples.

Country-specific Fintech definitions, for example as part of a national strategy, may go further to refer to the relevant policy objectives as well as the relevant financial functions subject to reforms. Holistic Fintech frameworks or model taxonomies can provide a vantage point for countries to narrow the relevant scope of Fintech in a national context.

6.1.3 Vision for Fintech

Informed by diagnostic studies and motivated by overarching financial and non-financial policy objectives, a clear vision for Fintech in a country will provide the foundation for regulatory reform to support Fintech innovation. 'It is typically a concise, inspirational and aspirational statement that defines medium- to long-term goal(s) of the strategy [not to be confused with the overarching policy objective].'[21]

Pro-innovation regulatory approaches can promote competition in financial services. However, not all types of innovation are equally important or be in demand. Given usually limited resources, policymakers and regulators will need to answer why – besides economic growth as an overall consideration – they want certain Fintech innovations, focusing on very specific parts of the Fintech universe.

A practical approach is to develop a nationally endorsed Fintech vision shared by a broad range of stakeholders, including government, regulators, private sector actors and others, which lays out the policy objectives that guide the implementation of policies, reforms, and investments. For instance, some countries will seek to strengthen financial inclusion, while others will seek to respond to international expectations around enhancing integrity.

The vision will identify the sector or services where innovation will most likely fall on fertile ground, i.e. where a focused political and financial investment will lead to quick, and long-term, impact. For instance, in a country where formal financial inclusion is low, Fintech policy could focus on financially including people in certain regions or market segments. In contrast, where the payment sector is mature and most people have a bank account, Fintech policy can seek to promote more sophisticated services, such as unemployment insurance.

The vision for Fintech can be expressed in a National Fintech Strategy which guides stakeholders and provides a basis for monitoring progress.

20 AFI, Mobile Financial Services: Supervision and Oversight of Mobile Financial Services (MFSWG Guideline Note No 12, 14 February 2014).

21 AFI, National Financial Inclusion Strategies: Current State of Practise (FISPLG Report, June 2018) 10 <https://www.afi-global.org/sites/default/files/publications/2018-06/National%20Financial%20Inclusion%20Strategies.pdf>.

Box: National Fintech Strategy (NFTS)

Enabling Fintech innovation in the financial system in a safe and secure manner for a defined policy objective requires a deliberate and coordinated approach to identify key opportunities and challenges, strengthen linkages and coordination across financial and non-financial domains, and align the efforts of a wide range of public, private, and civil society stakeholders.

A National Fintech Strategy (NFTS) can serve as a policy instrument to actively promote Fintech innovation to support increased competition or inclusion in the financial system while putting in place the necessary safeguards to ensure financial stability, integrity, and consumer protection, i.e. to balance the range of financial (and non-financial) policy objectives.

An NFTS document is informed by evidence and prepared in consultation with stakeholders. It can be a useful tool to provide a common definition of Fintech, to chart a clear vision for Fintech, to outline strategy objectives, to identify Fintech drivers, challenges and opportunities for policies, reforms, and investments across the ecosystem. It can help to effectively coordinate actions and allocate needed resources in priority areas in view of the set policy objective(s).[22]

Forthcoming Guidelines for National Fintech Strategies by the Arab Region Fintech Working Group will provide country stakeholders with specific assistance and recommendations.

Suggested Resources

- AFI, Fintech for Financial Inclusion[23]
- CGAP, Four basic regulatory enablers[24]
- IMF, Bali Fintech Agenda[25]
- G20, High Level Principles for Digital Financial Inclusion[26]
- UNSW, Regulatory Handbook: The Enabling Regulation of Digital Financial Services.[27]

6.1.4 Governance and Institutional Coordination

a) Coordination is Required Across Public, Private, and Civil Society Stakeholders

Turning vision into reality requires an appropriate, effective framework to coordinate policies, reforms, and investments.

The main participants in developing legislation include relevant regulators and government entities. The legislature will be involved where Fintech reform includes formal amendments to legislation. Promoting financial inclusion through Fintech can involve a range of departments and regulators, including ministries of economy, industry and trade, education, IT and communications, and financial, competition and telecommunications regulators. Ambiguities or overlaps in regulatory jurisdictions can result in conflicting regulation or weak enforcement. For instance, the financial regulator may identify competition or data privacy concerns with Fintech which may require action from other regulators.

Private sector participants (service providers, industry, consumer organisations and research facilities) are often important. A timely, regular, consultative process among public, private, academic and civil society players can enhance knowledge and enable technological and financial services innovation.

We recommend implementation of Principle 6 of the G20 Principles for Innovative Financial Inclusion,[28] by ensuring cross-sectoral coordination through a national governance framework with an inter-agency coordination structure (which

22 AFI, National Financial Inclusion Strategies: Current State of Practise (n 22); EY (n 4); IMF and World Bank, The Bali Fintech Agenda (Chapeau Paper, 19 September 2018) ‹http://documents.worldbank.org/curated/en/390701539097118625/pdf/130563-BR-PUBLIC-on-10-11-18-2-30-AM-BFA-2018-Sep-Bali-Fintech-Agenda-Board-Paper.pdf›; World Bank, Developing and Operationalizing a National Financial Inclusion Strategy (Toolkit, June 2018) ‹https://openknowledge.worldbank.org/bitstream/handle/10986/29953/NFIS%20Toolkit.pdf?sequence=5&isAllowed=y›; World Bank, Template for the Design of a National Financial Inclusion Strategy (Template) ‹http://www.meridian.org/wp-content/uploads/2016/12/Template-for-the-Design-of-a-National-Financial-Inclusion-Strategy_by-the-World-Bank-Group.pdf›.

23 Arner, Buckley and Zetzsche, Fintech for Financial Inclusion: A Framework for Digital Financial Transformation (n 13).

24 Stefan Staschen and Patrick Meagher, Basic Regulatory Enablers for Digital Financial Services (CGAP Focus Note No 109, May 2018) ‹https://www.cgap.org/sites/default/files/researches/documents/Focus-Note-Basic-Regulatory-Enablers-for-DFS-May-2018.pdf›.

25 IMF, The Bali Fintech Agenda (Policy Paper, 11 October 2018) ‹https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/10/11/pp101118-bali-fintech-agenda›.

26 GPFI, G20 High-Level Principles for Digital Financial Inclusion ‹https://www.gpfi.org/publications/g20-high-level-principles-digital-financial-inclusion›.

27 Malady, Buckley, and Tsang Regulatory Handbook: The Enabling Regulation of Digital Financial Services (UNSW Law Research Paper No. 2016-05) ‹https://ssrn.com/abstract=2715350›.

28 'Cooperation, Create an institutional environment with clear lines of accountability and coordination within government; and also encourage partnerships and direct consultation across government, business, and other stakeholders.'

can take the form of a formal agreement or Memorandum of Understanding [MOU]),[29] and a defined lead agency. The role of each regulator and party should be clear, and the framework should evolve as the process matures.

b) Responsibility for Leading Fintech Reform Should be Assigned to One Institution

Experience suggests strongly that an efficient reform process needs one institution to lead, drive and coordinate it. This could be the office of the President, the Ministry of Finance or the Central Bank, and is, most often, the Central Bank. This lead institution should set goals and facilitate the coordination of the range of processes required to support the growth of Fintech and financial inclusion.

c) Coordination is Required Within Authorities

Fintech is often addressed in a range of departments within one regulatory authority, including payment, securities and lending departments. Accordingly, collaboration within the authority is vital. Fintech reform is further likely to require expertise from IT, legal, research and (where they exist) non-bank financial institutions departments.

Coordination is key both for leveraging the authority's in-house expertise, and for creating the necessary consensus across the authority. For example, while the banking supervision department might generally be in charge of licensing and approving new providers and products, the IT department may have the expertise to promote cybersecurity.

In many countries **financial inclusion 'units'** are responsible for executing the overall reform strategy.[30] An alternative is an internal financial innovation / Fintech committee that spans departments of the financial regulator.[31]

GIZ experience suggests that such units or internal committees that include representatives from all relevant departments are effective. The committee should have the necessary power to make recommendations on all aspects of digital financial services / Fintech, e.g. draft regulatory texts, licensing, approval, and research. This should ensure an efficient policy development and implementation process.

Suggested Resources:

- AFI, Current State of Practise in Financial Inclusion Strategies[32]
- World Bank, Developing and Operationalizing a National Financial Inclusion Strategy[33]
- World Bank, Coordination Structures for Financial Inclusion Strategies and Reforms[34]

6.2 Smart Regulatory Approaches to Fintech Innovation

There are many ways a regulator can approach promoting Fintech innovation. These include supporting research and development; human capital development; marketing; investment promotion, including the establishment of investment funds; creation of incubators and accelerators; and legal and regulatory reforms. In this section we consider seven in particular: (1) abolition of unsuitable regulation, (2) proportional regulation, (3) innovation hubs, (4) testing and piloting, (5) regulatory sandboxes, (6) restricted licensing, and (7) waivers and no-action letters.

29 The International Telecommunication Union (ITU) Focus Group on Digital Financial Services (FG DFS) works on developing a model MOU, providing a template for information and communication technology (ICT) regulators and central banks to define and outline joint objectives and means of cooperation and collaboration. See ITU, ITU-T Focus Group Digital Financial Services Ecosystem (Report, 2017) 29-33 <https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-DFS-2017-PDF-E.pdf>.

30 Examples include regulators in Nigeria, Uganda, Mexico, the Philippines and Indonesia as well as the European Securities and Markets Authority (ESMA).

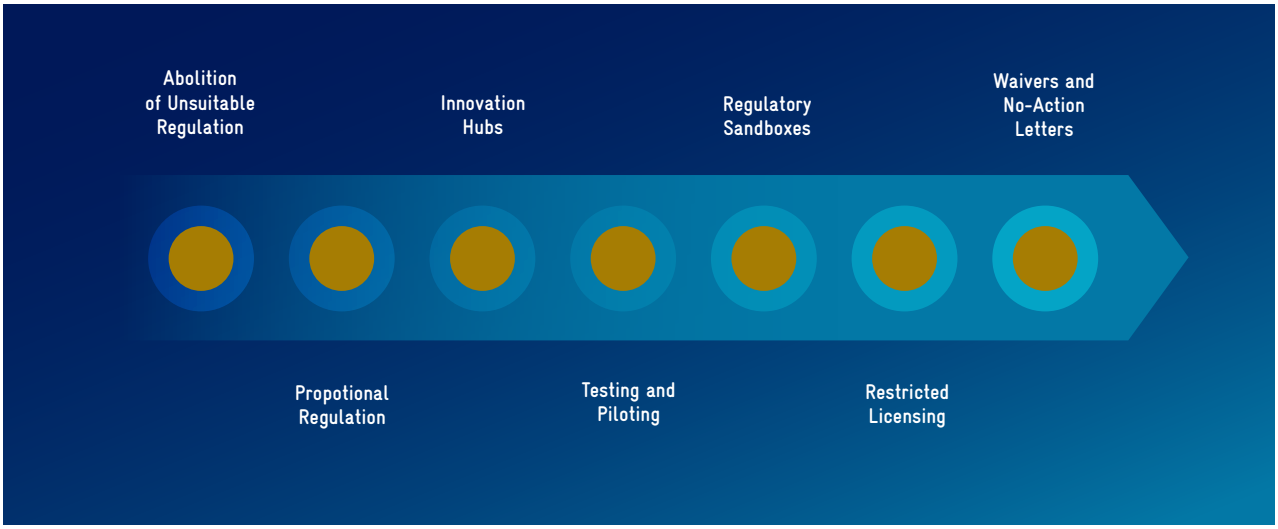
31 Examples include Tanzania, Malawi and Pakistan, cf. AFI, Mobile Financial Services: Supervision and Oversight of Mobile Financial Services (n 21).

32 AFI, National Financial Inclusion Strategies: Current State of Practise (n 22).

33 https://openknowledge.worldbank.org/handle/10986/29953

34 http://documents.worldbank.org/curated/en/350551468130200423/Coordination-structures-for-financial-inclusion-strategies-and-reforms

Figure 5 – Approaches to Promoting Fintech Innovation



6.2.1 Abolish Regulation (Red Tape)

Abolishing regulation is often a relatively easy and inexpensive approach. However, most rules were adopted initially for a reason. So before doing so, a regulatory impact analysis should determine whether the rule in question remains useful. Rules which are often ripe for abolition include formal requirements (such as rules asking for confirmation in writing or certified copies, as such information can often be confirmed today from other data sources including corporate registers, tax information etc.).

6.2.2 Ensure Proportionality of Regulation ('Bespoke Regulation')

Proportional regulation includes stricter rules for larger firms, and more lenient rules for smaller ones. Proportionality is key, alongside competition policy considerations, when devising formal and supportive pathways for Fintech start-ups into the market. Proportionality needs to be reflected particularly in regulations concerning market stability (including capital requirements) and market integrity (tiered KYC or CDD requirements depending on transaction size) to create an enabling playing field for new non-bank financial service providers. Some rules, however, don't lend themselves to this approach. For instance, it makes no difference to customers whether they have been defrauded by large or small firms, so fit and proper person tests for corporate officers should remain.

6.2.3 Innovation Hubs

An innovation hub is a unit within the financial regulator that serves as a portal through which industry can access regulators to discuss their Fintech innovation and obtain regulatory guidance or dispensations. An innovation hub itself does not require legislation. A hub is typically staffed by regulatory experts.

Regulators who wish to genuinely promote innovation need to make available the staff to interact with industry, where necessary, issue bespoke waivers or other forms of dispensation of some regulatory requirements and assist with advice and guidance to Fintech start-ups seeking to navigate the regulatory maze.

Innovation hubs will generally be the most efficient and effective regulatory approach to promote and facilitate innovation in financial services, while sandboxes – more expensive to set up and maintain – tend to attract the headlines and send an innovation-friendly message to the market.

6.2.4 Testing and Piloting Arrangements

Regulators can grant leniency (and exemption from licensing requirements) for testing and piloting, under a wait-and-see or test-and-learn approach.[35]

35 See eg Ivo Jenik and Kate Lauer, Regulatory Sandboxes and Financial Inclusion (Working Paper, CGAP, October 2017) ‹https://www.cgap.org/sites/default/files/Working-Paper-Regulatory-Sandboxes-Oct-2017.pdf›.

A wait-and-see approach is often advisable when an innovation is not a threat to retail consumers. A test-and-learn approach is defined by clear boundaries in terms of transaction volume and duration of the test – whether the activity is continued depends on the outcome of the test. In a pilot, in contrast, the intention from the outset is to continue the activity after the piloting period – which is designed to provide some data which is missing.

For testing and piloting applications regulators must define with certainty where testing and piloting ends and regular activity begins. Overall, these approaches enable innovation in the market, including in data collection, on a temporary basis within boundaries or with safeguards in place. They allow the regulator to monitor associated risks, thereby to inform policies and the decision-making for regulatory reform or to identify sectoral gaps that merit further attention. An exemption for testing and piloting is particularly useful for authorized financial institutions as they can test new technology and business models under their existing licence.

Where an activity meets the definition of a regulated activity, pursuing it cannot be justified on testing and piloting grounds unless (1) the clients are not selected on actual market criteria—we refer to this category as "fake clients"; (2) the test participants are aware of their guinea pig function; (3) the use is limited to a certain number of occasions, a specific time, or certain clients; and (4) the testing environment is insulated from the licensed entities' or Fintechs' "real" business activity. Where clients consent, the Fintech could justify testing and piloting for some time.

6.2.5 Regulatory Sandboxes

Regulatory sandboxes are safe spaces in which Fintech start-ups and other innovative enterprises can develop and test their innovations without being subject to the full extent of financial regulation. A sandbox is a tightly defined safe space which automatically grants relief from some regulatory requirements for those entities that meet its entry tests. In contrast to testing and piloting, the sandbox requires formal approval of entry by a regulator. The sandboxed firm does not, at first, get an unlimited licence. Its right to pursue the activity is conditioned upon its remaining in the sandbox, and statutes tend to limit sandbox participation to anywhere between 6 and 24 months.

One upside of both sandboxes and innovation hubs are the learning outcomes for the regulator from the close interaction with innovative firms. One downside, especially of sandboxes, are possible conflicts of interests which may arise when a supervisory agency, having 'sandboxed' a firm for a while, has an interest in it being a success story. Additional concerns relate to the rule of law, equal treatment of competitors, and the costs of establishing a sandbox scheme which may turn out to be incommensurate to the returns in terms of numbers of firms benefitting from a sandbox, in particular when compared to an innovation hub.

> "The U.K. FCA sandbox grew out of its innovation hub, termed Project Innovate. Likewise in Australia, the Australian Securities and Investments Commission's sandbox grew out of its innovation hub, which well preceded the sandbox. […] In cases where Fintech and innovation firms are emerging and presenting challenges to the existing regulatory regime's approaches, a sandbox may be a useful additional element of the Fintech and innovation ecosystem."[36]

36 Ross P Buckley et al, 'Building Fintech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond' (Working Paper No 53, European Banking Institute, 1 November 2019) ‹https://ssrn.com/abstract=3455872›.

Egypt has adopted a regulatory sandbox framework in June 2019. As of December 2019, 3 firms benefitted from Sandbox testing.

The Regulatory Sandbox in Egypt is a cohort-based business model: only Fintech companies and start-ups specializing in the subject announced at each cohort are accepted in the selection process. The first cohort 2019 was based on Fintechs specializing in e-KYC solutions.

The number of Fintechs accepted to the program may vary at each cohort depending on resources and capabilities. This allows keeping adequate guidance and supervision standards.

Participants need to meet six eligibility criteria: the innovation must be
1) within the Fintech scope,
2) genuinely innovative,
3) provide a benefit to customers,
4) must be in a real need for the Regulatory Sandbox,
5) be a mature solution, and ready for Sandbox testing and
6) support digital transformation & Financial Inclusion initiatives.

A separate team within CBE coordinates the Regulatory Sandbox in Egypt and it follows a defined process, which includes the following phases:
1) Application stage. Among the documents required for the application, applicants need to provide a detailed testing plan that would eventually need to be integrated and approved by CBE if successful. Testing plans include among other things, risks associated with the business, caps and floors for the number of clients as well as the value of transactions, etc.
2) Evaluation Stage.
3) Preparation stage. In this phase, the applicant must select and provide a list of customers, who need to be aware of the risks incurred by making use of the services/technology offered by the sandboxed company (formal consumer protection terms).
4) Experimentation stage. Upon selection, Fintechs are accepted to the Regulatory Sandbox for testing. Within the Regulatory Sandbox, Fintechs may operate freely, testing their technology with real clients over a period of 6 months (an extension up to 12 months is allowed). Sandboxed firms must fulfil some reporting requirements, primarily a monthly progress measured across different KPIs and optionally they can provide a report listing operational or technical incidents, audits and customers satisfaction reports. The objective of regulators is to collect, through reporting, statistically relevant parameters in order to measure the impact of the services provided by the sandboxed Fintechs in the ecosystem and to evaluate their growth.
5) Exit. In the event of success, the sandboxed firm is allowed to enter the Egyptian financial market, after obtaining a licence if required.

Even if Fintechs are not required to have their activities backed by a traditional financial institution, most of the applicants had partnerships with banks.

The regulatory Sandbox in Egypt is part of an articulated Fintech vision and strategy, which was developed after an accurate assessment of the national ecosystem aimed at identifying specific local challenges. These assessment considerations are directly translated in the selection procedures and functioning of the Regulatory Sandboxes. For instance, the assessment revealed that 99 % of the ventures in Egypt are SMEs and it was reported in our survey that Fintechs that target SMEs are preferred in the selection process compared to other Fintechs targeting different client segments.[37]

37 https://fintech-egypt.com/sandbox/; own survey and interview.

In summary, the real work of promoting Fintech is far more likely to be done by an innovation hub than a sandbox. Sandboxes, for reasons of consumer protection, must have narrow entry criteria. Innovation hubs merely facilitate interaction with regulators for the purpose of receiving guidance and possibly dispensations. For this reason, the number of providers that typically benefit from an innovation hub far eclipse the number that qualify for a sandbox.

However, our recommendation is for regulators in the MENA region to have both a sandbox and a hub. This is because the sandbox term cuts through and having one tends to send the clear (and valuable) message that the regulator is flexible and easy to deal with. This is probably because many jurisdictions now have sandboxes and nearly all use that term in describing them. Fewer jurisdictions have innovation hubs and use a wide range of names for them. So, the term 'sandbox' will cut through, while the actual work of promoting innovation is far more likely to be done in the hub.

6.2.6 Restricted Licensing

Restricted licensing enables the grant of partial licences. For instance, a wealth management firm could be licensed to provide investment advice for liquid financial instruments to wholesale clients only, rather than being licensed to advise wholesale and retail clients on all asset classes. A payment institution could be licensed to provide simple retail payments only. The ASIC Fintech licence grants a licence swiftly to innovative firms which meet the criteria. The upside of restricted licensing is legal certainty and transparency and reduced costs for entrepreneurs, while downsides include that strongly growing firms may quickly outgrow the restrictions.

ASIC Fintech Licensing Process[38]

- Fintechs that are required to obtain an Australian Financial Services (AFS) licence, or a credit licence, need to undergo the regular application process, common to all AFS and credit licences applications
- However, the licence can be tailored to the particular circumstances of the applicant and the applicant only needs to apply for relevant authorisations - so if the Fintech only offers two types of financial services, it only needs to apply for a licence for those two specific activities, and does not need to apply for a full licence
- The application process is thus simplified
- Further, some activities are exempt from licensing requirements, e.g. provision of general advice, only providing referral services etc[39]

6.2.7 Waiver and No-Action Letters

With waivers, authorities assess conduct on a case-by-case basis and declare, at the end of a formal proceeding, whether certain conduct is deemed to comply with the law, even though it may in some respects not comply with all details of a written rule. The waiver / no-action letter approach differs from the "wait and see" approach since the supervisory authorities take an active decision to tolerate a certain conduct (i.e. they may assume liability, if the law provides for liability in cases of unlawful waivers). Waivers and no-action dispensations are most often extended to licensed institutions, but the practice can usefully be applied to Fintech start-ups.

For rule of law reasons, the procedures for waiver / no-action letters should follow certain internal guidelines, and the outcomes should be published, to ensure other firms can seek the same degree of regulatory lenience. Firms applying for no-action letters should be required to provide a factual brief and a legal assessment which discusses the rules and explains why disregard of certain aspects of the rules is in line with the ISIP taxonomy laid out above.

38 See 'Fintech Licensing FAQs', ASIC (Web Page, 15 January 2020) <https://asic.gov.au/for-business/innovation-hub/asic-and-fintech/fintech-licensing-faqs/>.

39 See Australian Securities and Investments Commission, Licensing: Financial Product Advice and Dealing (Regulatory Guide 36, June 2016).

Insights From the MENA Region

No-Action Letter Practice

1 out of 6 countries make use of no-action letters but does not issue no-action letters often.

Fintech Waiver Policy

6 out of 6 countries do **not** have a Fintech waiver policy. 3 out of 6 countries would consider changes to the law in this regard, while 3 want to retain their approach.

6.2.8 Umbrella Licence

The umbrella licence is granted to a business that meets the licensing requirements of a given country, yet performs the regulated activity by way of outsourcing. The Fintech firms are delegates of the umbrella licence holder. An umbrella licence creates economies of scale for costs of regulation and supervision since only the umbrella licence holder needs to report to supervisory authorities, pay licensing fees (if any) and ensure compliance with the regulations.

While attractive for small Fintech firms, the Umbrella licence holder also assumes liability for misconduct by the Fintech firms. This could result in a perverse incentive structure where the benefit of misconduct is allocated to the Fintech firm and the costs / liability to the Umbrella-licence holder.

A case where umbrella licences may be useful may involve tech-cluster and accelerator providers where the provider sets the conditions for and selects participants in the cluster / accelerator and subjects them to its contractual conditions. An umbrella licence could be fruitful particularly to secure proper performance of certain key compliance concerns, in particular KYC checks to control AML / CTF risks, as well as financial and operational risk management. An umbrella licence requires, on the side of the licence holder, a sophisticated control and reporting infrastructure as well as seasoned key management.

6.2.9 Voluntary Fintech Licences

Several firms that are not yet licensed in the MENA region understand a licence as a benefit when contracting with larger banks, yet licensing is restricted to firms pursuing a certain regulated activity, with the scope of regulated activity being rather traditional and limited to archetypes of financial intermediation. These firms could consider submitting themselves to a voluntary licensing process, despite the fact that they do not pursue one of the archetype financial services, in order to benefit from the positive effects that they expect from a regulatory approval in return for submitting themselves to reporting requirements and regulatory oversight. Examples could include the provision of AML / CTF checks or data analysis/ scoring on behalf of regulated intermediaries.

While we note that a "voluntary" Fintech licence would be novel, in an environment like the MENA region where regulated activities are often not granularly written in the respective law a voluntary Fintech licence could yield some benefits, yet the limits and legal consequences of such a voluntary scheme would need to be clearly defined.

6.2.10 Regional Fintech Licences

For mid-size firms the small geographic scope of a banking or financial services licence is a disadvantage since these firms lack the size to establish subsidiaries, and acquire licences, in each country of the MENA region. These firms would welcome a regional licensing scheme, similar to the European Passport covering all EU and EEA countries.[40]

As the European experience shows, expanding a national licence into a regional licence requires a significant degree of harmonization of laws across the region in addition to close cooperation and trust among competent authorities in the region, paired with some oversight mechanism to avoid arbitrage.

40 For further information on the European passport and access requirements across regions see Dirk A Zetzsche, 'Competitiveness of Financial Centers in Light of Financial and Tax Law Equivalence Requirements' in Ross P Buckley, Emilios Avgouleas and Douglas W Arner (eds), Reconceptualising Global Finance and its Regulation (Cambridge University Press, 2016) 390.

6.3 Market Approaches to Fintech Innovation

Non-legal systemic interventions for financial innovations include strengthening the demand side, strengthening the supply side, and furthering innovative entrepreneurship. These non-legal interventions also include:

1. enhancing financial and tech literacy programmes,
2. supporting cybersecurity research centres (regional or national), to address cybersecurity risks through a collaborative approach.

Jordan's cyber security policy foresees:

- the creation of national Computer Emergency Response Teams (CERTs) to deliver continuous network monitoring and threat intelligence and incident response capability,
- a cyber-training programme to enhance the skills of NCP stakeholders and CERT staff;
- Public Key Infrastructure (PKI) to manage secure information communication, and identity authentication and digital signatures;
- an international information security co-operation programme to aid information sharing, exchange lessons learned and enhance capability development.[41]

3. supporting accelerators by a) tax incentives for R&D, b) government-provided office space, and c) university excellence programmes in the STEM sector,
4. attracting angel investors by a) tax incentives for R&D, and b) innovation fairs and events,
5. supporting the development of tech / digital clusters (university – private – government), by a) designating and subsidizing office space close to universities for Fintech firms, and b) ensuring presence of supervisory agencies in that designated space, for instance by having a branch there of the innovation hub through an ongoing contact office for initial advice on regulatory matters at least say two days per week,
6. supporting alternative career paths of tech entrepreneurs with start-up grants, entrepreneurial awards, tax incentives for R&D,
7. promoting tech (cybersecurity) cooperation and standardization among intermediaries in order to enhance cybersecurity while reducing its costs, and
8. creating digital clusters (for instance, around universities) to further regional technology expertise. Similar to financial centres, these digital centres could develop services which are not available or too expensive to build, while ensure sufficient customization to the local context. The cost-benefit analysis of a digital centre strategy is particularly important to ensure wise spending of public funds.

6.4 Furthering Digital Finance by Other Means

Regulators can further tech implementation among financial services firms through rules that lead to pro-innovation investments by way of digital reporting requirements, data privacy and liability rules. The interaction of apparently separate reforms can drive the development of digital finance.

6.4.1 Reporting Tools, Tech-Based Reporting

In tandem with post-crisis international regulatory approaches, many regulators (in particular in Europe) have imposed very extensive reporting obligations on financial intermediaries in an effort to combat systemic risk as well as address a range of integrity risks emerging from money laundering, terrorism financing and competition scandals. These financial regulatory reforms have a common focus related to international financial regulatory standards; and a common imposition of extensive reporting requirements upon the financial services industry. All in all, these reforms have spurred rapid digitization of finance, financial reporting and regulatory capacity digital finance, in the following way:

When faced with a proposed regulation, the financial services industry will demand sufficient time to build the necessary IT systems to implement it. The necessity of technological implementation of regulatory reporting requirements then forces intermediaries and their service providers to continually invest in the development of their software and IT systems to ensure sufficient data are collected within their organization to meet reporting requirements, that these data are packaged and reported in the necessary structure and form. This is the process of datafication: the application of analytics tools to digital data. Once financial intermediaries have "datafied" their reporting, the regulators and supervisors are also forced

41 See http://moict.gov.jo/uploads/studies/National%20Cyber%20Security%20Strategy%202018-2023.pdf

to develop data management systems, which are capable of receiving and processing the volume of data being generated and delivered by the financial services industry. With enhanced analytics tools, supervisors can handle even more data (and in turn, tend to ask the supervised entities to collect and transmit even more of it, triggering another Regtech cycle).

6.4.2 Data Privacy Rules

Another field of legislation driving technological progress includes the imposition of enhanced data privacy rules. Legislation could require financial institutions, for instance, to reorganize their data processing as well as client data policies to meet the requirements of data privacy legislation (with the EU's GDPR providing the most advanced example). The extensive details on personal data of individuals also require data categorization tools which allow for amendments and deletion after a given timeframe or upon the natural person's request. Financial intermediaries have often collected large amounts of data from and about their customers, over long periods of time. However, in many cases, these data have not been used effectively, because they have been restricted to certain business units, lines, products or silos within individual firms. Under data privacy rules, financial intermediaries are obliged to build comprehensive systems for their digitized data which address the collection, storage, use and protection of the data. The process of digitization combined with systemization to meet the data privacy requirements may trigger a revolution in financial industry treatment of customer data, in the same way that data-oriented reporting requirements drive a revolution in financial industry collection and processing of business and regulatory data. However, unlike the financial regulatory reforms which drive not only digitization but also datafication, data privacy rules create barriers to centralization of individual customer data and its use, placing requirements on the financial industry to develop new systems of data management and also shifting control of many aspects of their data from financial and data intermediaries (which have collected it) to individual customers (who are its subject).

6.4.3 Allocating Responsibility

Vulnerable people tend to lack financial and tech literacy. Legal language in contracts often works against them, allocating responsibility for misuse of their password, cyber risks, or abuse of their customer data to them rather than the service providers. This undermines trust in financial services and undercuts a crucial support for ensuring financial inclusion which is that clients use the services to which they have access.

Legislation can shift responsibility in these cases to the entity with best means and resources to fend off cyberattacks and bear the risks: the financial institution. It is typically the financial service providers that can best increase security and monitor clients' accounts and assets against attacks.

Rules promoting trust in financial services through allocating liability and responsibility to the "cheapest cost avoider" are widespread in modern financial legislation. For instance, the EU Payment Services Directive II (adopted in 2016*) allocates responsibility for regaining clients' assets from unauthorized payments entirely to the financial institutions. However, responsibility does little if the provider lacks the means to meet its obligations, so legislation could pair with liability with the requirement to either provide additional capital reserves or liability insurance for cases of mandated liability.

7 CONCLUSIONS

We have sought in this report to provide policymakers and regulators in the MENA region with guidance and the range of options available to them to harness Fintech innovation based on global best practice. The choice of any particular regulatory approach is of course a matter of sovereign discretion informed by the local expertise of the domestic ecosystem and market.

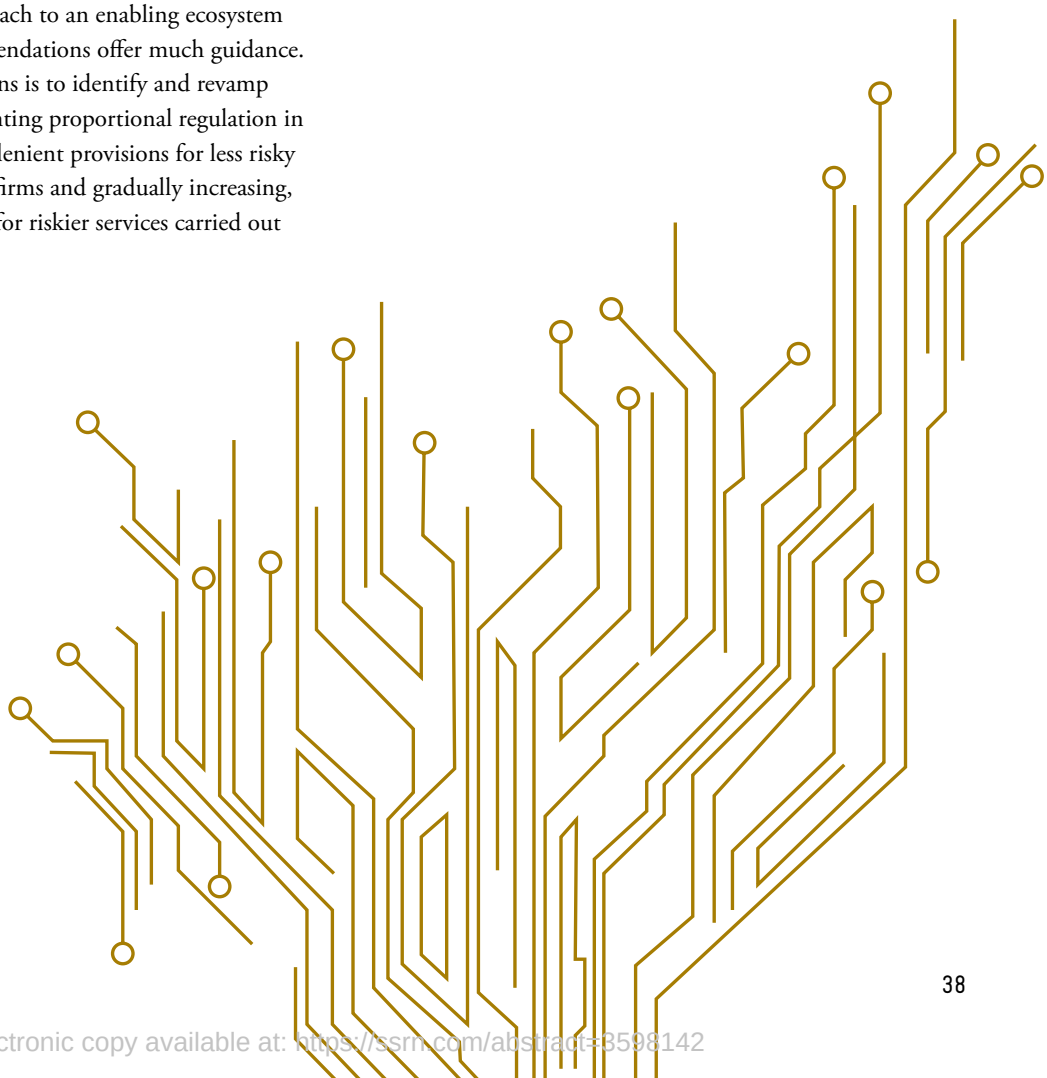
We suggest that policymakers and regulators, however, particularly pay attention to the benefits of regionally harmonized regulatory frameworks for Fintech. The more consistent regulatory approaches are across the region, the more attractive each of the national markets will be to innovative financial service providers. This is because consistent regulation facilitates the expansion and rollout of Fintech innovation across the region, enabling providers to materialize economies of scope and scale and clients to choose from a wider set of services.

Achieving regionally integrated framework conditions as part of enabling ecosystems for Fintech may not be an easy task. Stakeholders across the region are well served by realising that a high level of effortful collaboration is their best pick to attract on the global stage the innovative sorts of financial services providers. These will further Fintech across the entire MENA region with benefits for financial inclusion, competition and economic development at large.

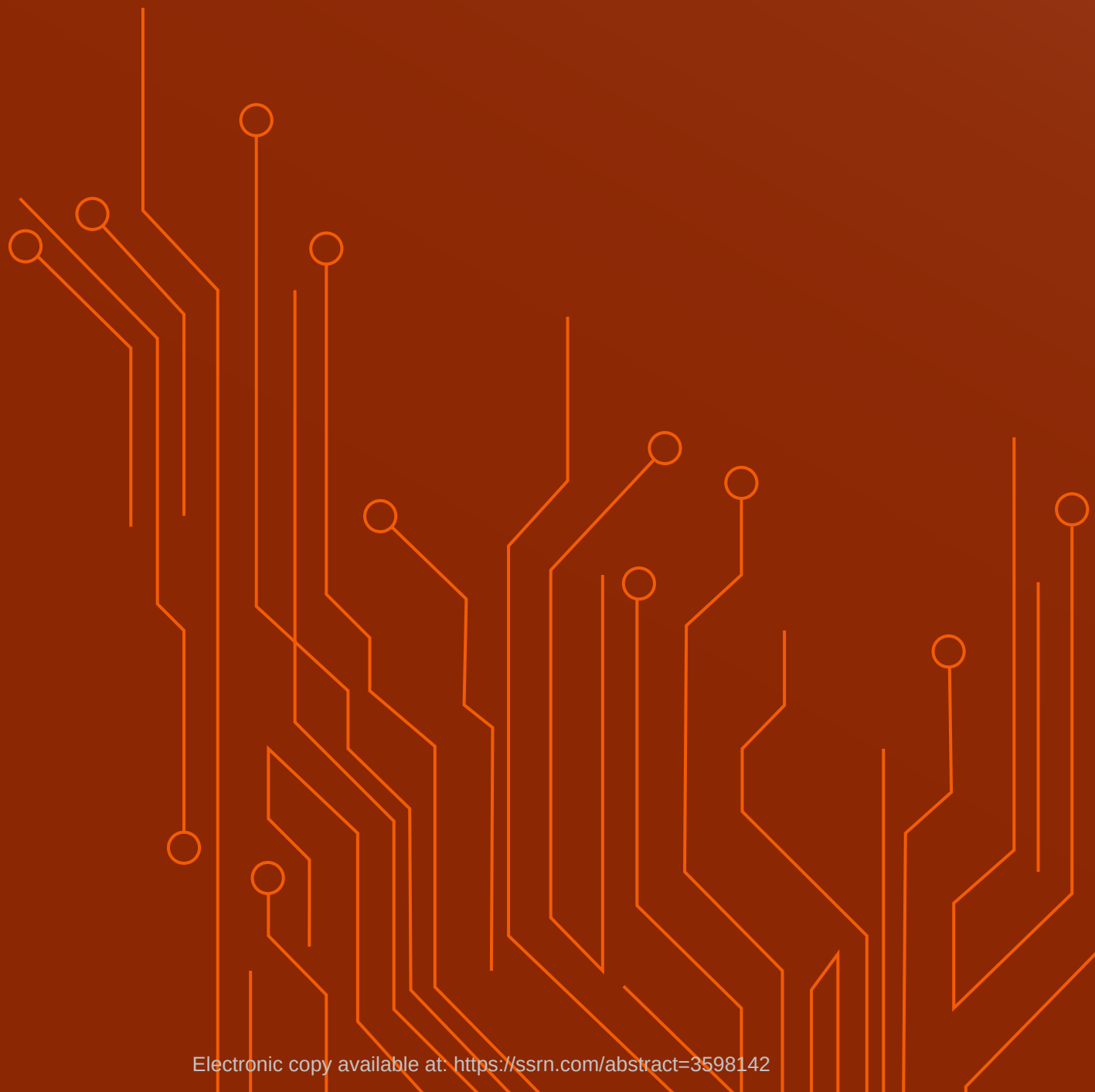
In pursuing this regional approach to an enabling ecosystem for Fintech, the above recommendations offer much guidance. A good starting point for nations is to identify and revamp legacy regulations by implementing proportional regulation in a tiered approach – with more lenient provisions for less risky activities such as by non-bank firms and gradually increasing, more prudential requirements for riskier services carried out by financial institutions.

We also suggest at the same time that financial regulatory authorities establish Innovation Hubs with staff that is knowledgeable of the financial licensing regime and encouraged to develop the capacities regarding Fintech developments and the local business environment. The Innovation Hub experts should be readily contactable by Fintech start-ups and financial institutions and able to provide guidance about regulatory requirements and dispensations.

Finally, subsequent reforms can include the establishment of a regulatory sandbox, as much for the message having a sandbox will send, as to the number of likely entrants into it. Global experience strongly suggests that most Fintech entrants in the MENA region will probably not qualify for a sandbox – or will decline to enter it, as their growth trajectory will take them quickly beyond the limits – but will benefit greatly from the guidance by an Innovation Hub.



ANNEX 1:
FINTECH-RELATED FINANCIAL STABILITY ISSUES AND POTENTIAL POLICY RESPONSES



1 Fintech-Related Financial Stability Issues

Prior to 2008, the regulatory focus was on identifying major risks and building appropriate regulatory and supervisory frameworks, principally through the Basel II Capital Accord. Basel II and financial stability regulation in general focused on a "micro-prudential" approach prior to 2008 in which regulators focused on the safety and soundness of individual financial institutions through such prudential regulatory standards.

This approach focused on five major categories of risk: credit / counterparty risk, market risk, payment risk, operational risk, and legal risk. Basel II included capital charges and related regulatory standards for the first four of these (with little attention to legal risk).

In this framework, risks relating to technological and data issues were included in operational risk, and thus attracted a relatively small cost in capital charges and related risk management and compliance systems. Since 2008, financial stability regulation has focused far more on 'macroprudential' risks. These risks arise from interdependencies in markets and were at the heart of the 2008 crisis. They have thus been central to post-crisis financial regulatory reforms.

With digital financial transformation, the standard post-2008 approach no longer addresses the full range of risks faced by a financial system. The emergence of digitisation and datafication means technology risks (including risks relating to cybersecurity and data privacy) should be seen as a separate form of risk, beyond traditional operational risk. Technology risks can arise within individual institutions and in the interconnections among institutions; and, more fundamentally, have the potential to impact financial sector confidence and stability directly.

Several key areas of concern arising from digital financial transformation include cybersecurity, data security and data privacy, new forms of financial institutions and new financial market infrastructures. Accordingly, an appropriate framework of analysis encompasses: (1) new sources of traditional forms of risk; (2) new forms of risk; and (3) entirely new markets and systems (including systems for regulation such as Regtech).

a) Cybersecurity

Cybersecurity has become a strong focus of financial regulators, governments and financial and tech firms globally. Cybersecurity is a very significant source of systemic risk, and a significant national security issue. Cybersecurity risk can thus be a new source of traditional risk and a new form of risk with potentially catastrophic consequences. While the weight of the international risks is significant, addressing them at a cross-border level is particularly challenging due to both financial stability and national security issues.

While regulators – nationally, regionally and internationally – are focusing attention on related issues, the wide range of actors and motivations are a challenge. Though financial institutions and infrastructure providers must focus significant resources and efforts on cybersecurity, the role of states and state-supported actors highlights the difficulties of pushing the entire burden onto the financial sector. Furthermore, the rise of Fintech exacerbates certain cybersecurity threats that are unique to the financial system, and its stability.

As a result of the increased state presence in cyber-activities (including cyberwarfare), states have to take a leading role in building systems to monitor and support key economic sectors – such as the financial sector – in addition to private and regulatory attention to issues of cybersecurity.

b) Market Structure

Another major stability concern stems from the market structure and competitive efficiency of Fintech markets, especially the risk of market concentration. Technology is characterised by scale economies and network effects (where existing users of an application benefit from additional users). For instance, where many online traders use the same platform, all can benefit from intra-platform liquidity by cutting out third-party clearing and settlement. These effects also benefit the platform provider who thereby facilitates both trading and clearing and settlement. This highlights to real potential of technology platforms to turn into sectoral monopolists, with the finance industry becoming an oligopolistic structure with a few multi-service-platforms providing almost all services entirely inside the platform (and some external providers attached to, and entirely dependent upon, the platform). Likewise, data-driven technology industries are characterised by a lower degree of contestability. The more data necessary to compete in a Fintech submarket, the harder is entry for new firms. These market concentration and contestability issues will turn into a market composition issue over time. New entrants will be side-lined by data-rich technology firms (Bigtechs) entering finance. This will both reduce the innovative potential of Fintech markets, and enhance too-big-too-fail (TBTF) systemic risk.

In considering these issues, the *Financial Stability Board* (FSB) concluded in 2019, addressing Fintech and market structure:[42]

- To date, the relationship between incumbent financial institutions and Fintech firms appears to be largely complementary and cooperative.

42 FSB, Fintech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications (Report, 14 February 2019) <https://www.fsb.org/wp-content/uploads/P140219.pdf>.

- The competitive impact of Bigtech may be greater than that of Fintech firms. Bigtechs typically have large, established customer networks and enjoy name recognition and trust.
- Reliance by financial institutions on third-party data services providers (e.g. data provision, cloud storage and analytics, and physical connectivity) for core operations is low at present but warrants ongoing monitoring.

Since the time of that summary however, the rapid growth in cloud and data services raises a range of concerns.

c) Data Protection and Security

The increasingly central role of data in finance highlights a second major area of concern: data protection. Different approaches are developing in different economies, in part representative of fundamentally different societal approaches, with the US, China and EU exemplifying diverging legal approaches to use, ownership and protection of data. These various approaches raise major questions about the role of data in digitised and "datafied" societies and economies: who owns and controls data, and what does ownership and control entail? The EU's *General Data Protection Regulation* (GDPR) is the most ambitious, harmonised legal approach and reflects concerns for individual privacy (and thus grants rights to data subjects against data comptrollers).

In looking at related issues, it is important to distinguish between data security or protection risks and data privacy risks (about the collection and use of personal data, particularly where there are extensive privacy protections such as GDPR). Some governments have worked of late to adopt approaches similar to GDPR; a noteworthy example is India that follows a pro-technology approach paired with EU-style individual data protection rights and a state monopoly on crucial building blocks for the financial system. Nonetheless there remains wide variations in national approaches and capacities for data protection.

d) Infrastructure

In addition to new risks from the digital environment (particularly relating to cybersecurity and data protection and privacy) and from new financial institutions (particularly scale and network effects), new risks also arise from new forms of digital financial infrastructure. Bigtech has played a particularly salient role in this development. The activities of these firms are rapidly expanding into credit provision, insurance, and investment services, creating complex interconnected webs across several sectors.

Concerns about financial infrastructure are by no means new, with financial regulation focusing on payment systems since the failure of *Bankhaus Herstatt* in 1974 and on securities clearing and settlement systems particularly since the failure of the Hong Kong stock and futures exchanges in 1987, with both addressed by the *BIS Committee on Payment and Settlement Systems* and the *International Organisation of Securities Commissions* (IOSCO). Since 2008, the focus on 'financial market infrastructures' (FMIs) has increased dramatically, with leadership by the FSB and the renamed joint BIS-IOSCO Committee on Payment and Market Infrastructures. Since 2008, there has been an ongoing debate about whether the benefits of central clearing houses in reducing counterparty risk are exceeded by new risks of concentration and systemic reliance.

Cybersecurity issues arise directly with central counterparties (CCPs) and similar infrastructures. There are also TB2F / too-connected-to-fail (TC2F) concerns, particularly as new entrants use new technologies like blockchain or stablecoins to disrupt existing markets and participants.

We also see the emergence of new forms of digital financial infrastructure, particularly in cloud services. Cloud services and cloud service providers are playing an increasing role in the financial sector. This is particularly so with new Fintechs which are often cloud natives, with their entire business cloud-based. Traditional financial institutions are also increasingly using cloud services to backup existing systems and build new systems (often to replace existing outdated core systems based on old mainframes running seriously out-of-date software). These third-party service providers expose the financial intermediaries using their services to operational risks, and in particular to cyber-risks. This includes services supplied by the large IT service platforms to which many financial intermediaries are outsourcing core functions.

Financial supervision typically does not apply to the Big Data providers. IT/data providers usually fall outside the scope of financial regulation and financial regulators lack information about such firms and their potential roles in interconnectivity across the financial sector as well as tools of supervision or regulation.

Financial law usually responds to risks created by non-supervised firms by imposing strict outsourcing requirements on financial firms. In particular, the financial firm needs to ensure systemic stability at all times, regardless of the outsourcing of information technology. But how should a bank (even a JP Morgan or Goldman Sachs) ensure that a major tech company (for example Amazon, Apple, Google or Microsoft) provide appropriate service? Banks may struggle to police firms whose market value is many times their own, nor can they really ensure that Bigtech's cloud centres work.

Such issues about cloud services are leading to increasing discussion of whether such firms should be regarded as systemically important infrastructure providers and regulated accordingly, in the same way as are certain payment systems or securities / derivatives CCPs. Related discussions are also underway about whether cloud services are in fact a form of utility and need to be separated from other technology businesses.

The alternative to control of the service provider is diversification. For instance, financial law could require financial firms to have mirror cloud servers from three separate and unrelated providers. While mandatory diversification ensures some additional security and has some positive effects on market structure in the provider market, it attracts increased costs and other problems.

The first other problem is cybersecurity. The more financial data more providers hold, the greater is the risk of data corruption (stealing, manipulation or abuse) from inside or of a cyber-attack from outside. On top, digital financial services tend to use legacy or natively insecure devices, infrastructure and protocols that were originally built for communication data, not to guarantee the security of financial transaction data.

Second, mandatory diversification of data streams and server space reduces the benefits of datafication. It slows down IT processes and risks confusion: storing data on a blockchain using many different cloud-service providers costs time and resources. If a brokerage system runs on three different data systems simultaneously, which don't correspond, which of the three datasets is correct? These risks are exacerbated by the high concentration of the market for cloud storage and analytics. Financial intermediaries will have little choice. Other examples come from reliance on a small number of data providers, which in turn raises risks due to similarities of business models (as occurred with securitisation prior to 2008) and concentration and reliance risks.

2 Stability-Related Policy Tools

The deficiencies in the regulatory system with regard to global technology risks are similar to those deficiencies which contributed to the 2008 Crisis. They include loopholes in regulation, lack of coordination among regulators, information asymmetry, lack of expertise on the part of financial intermediaries and regulators, and lack of awareness or investment on the side of intermediaries.

First, in implementing strategies, regulators must prioritise tech risks, both internally and externally. The result should be that tech risks are treated as being as important as financial risks. This is particularly important in monitoring these new sorts of risk and collecting non-traditional forms of information. This could be done by appointing a Chief Technology Risk Officer (CTRO) for the supervisory authority in order to emphasise the significance of these sorts of risks. Financial intermediaries should also be required to appoint CTROs or equivalent senior management officers responsible for cyber, technology and data risks, as a main contact point, with board monitoring, at the least in the context of firms' risk committees. Further, the CTRO's report on cyber risk should be a core agenda item at all meetings of both the authorities and of the intermediaries' senior management.

Second, regulators need to strengthen in-house tech expertise to understand the sources of these new risk exposures of the ecosystems they monitor and supervise, and to be able to discuss tech matters with intermediaries.

Third, regulators must continue to enhance reporting requirements about the intermediaries' tech risk management strategies and the budget and human resources devoted to systemic stability and cybersecurity. These reports should include technological details and be read by the supervisor's tech department.

Fourth, regulators must prioritize these sorts of risks in both on- and off-site supervision to understand whether intermediaries have understood those risks and how they address them; and speak to IT staff as well as to upper management or the legal department during examinations. For the authorities both technology and regulatory experts should be present.

Fifth, regulators must strive to depoliticize cybersecurity where related to financial stability, to foster the development of intergovernmental or sectoral networks capable of preventing and defending against cyber incidents, especially considering the growing financial interconnectedness. An isolated cybersecurity island that is still connected to the "datafied" financial network poses increasing risks of contagion.

Sixth, regulators will have to make use of new technologies themselves, since only the user understands the issues with the application. This can be part of a major Regtech strategy which – in many instances – is overdue, in order to respond to the enormous data streams regulators receive in response to GFC-related additional reporting requirements. Regulators may also suffer from failures of technology, but if they do they will also learn to handle large tech projects – and know what they have to ask for from the intermediaries.

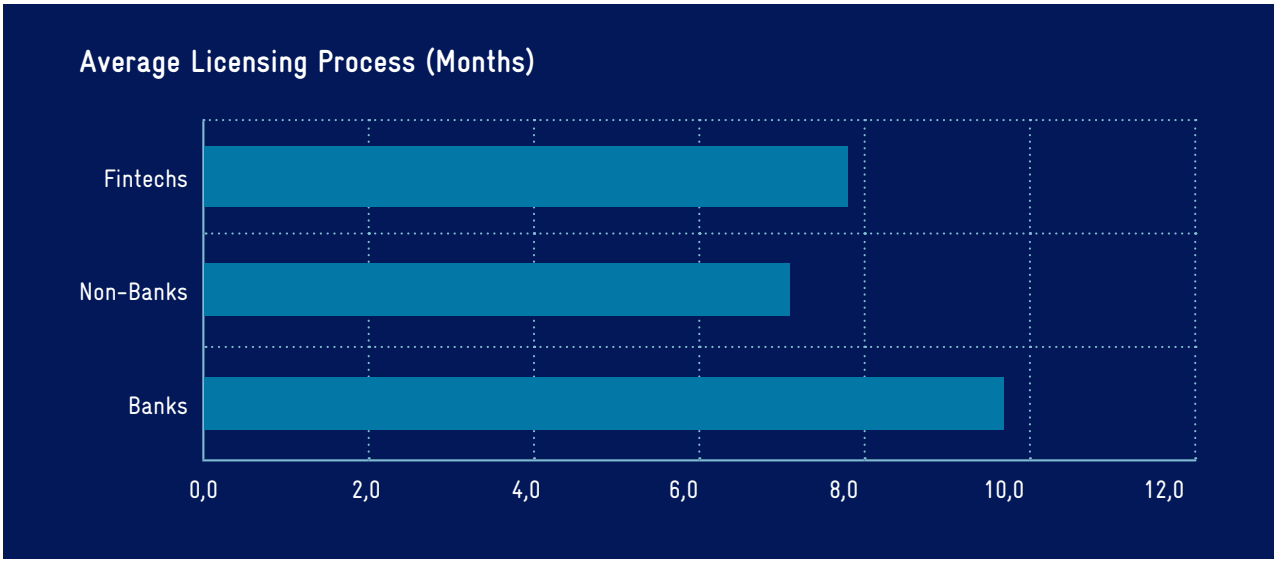
Seventh, regulators should continually seek to harmonise cyber and data policies to avoid friction and uncertainty, and not allow rules with potential impacts on financial stability to become entrenched. This may prevent races to the bottom that can intensify destabilising behaviour.

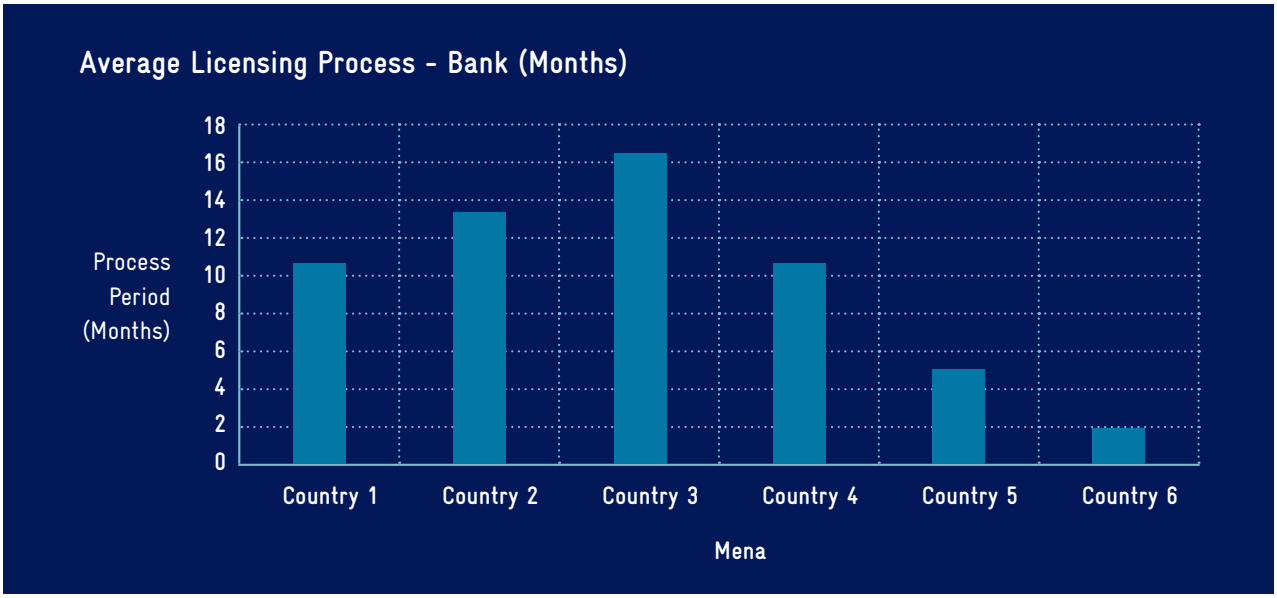
ANNEX 2:
INSIGHTS FROM THE MENA REGION

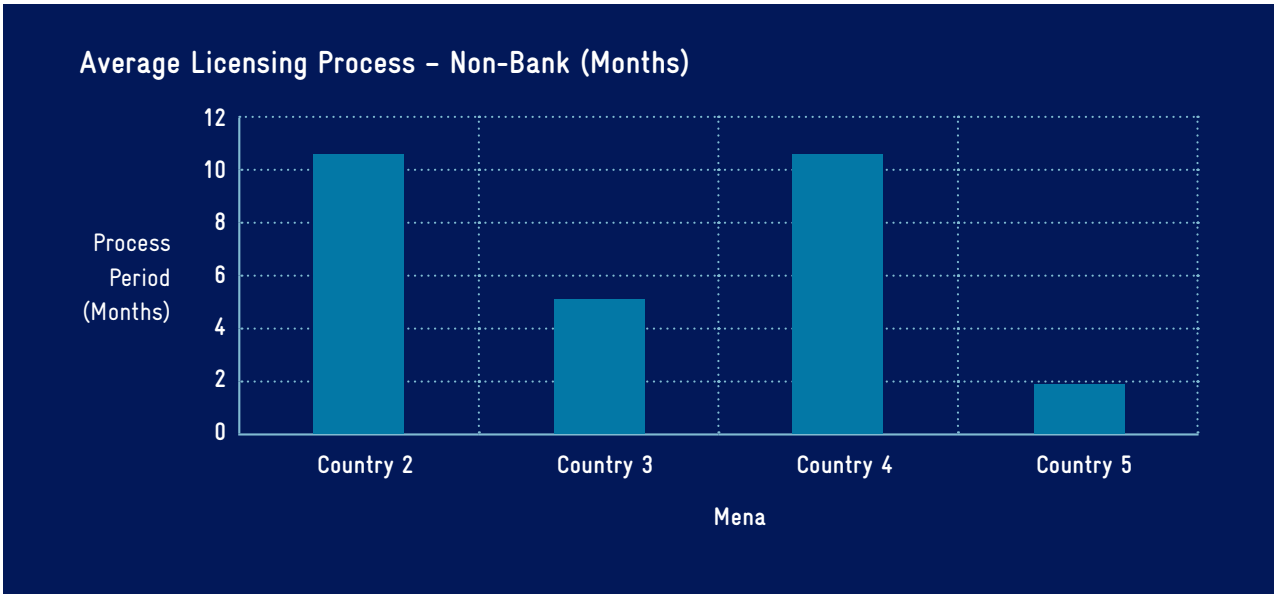
Insights From the MENA Region

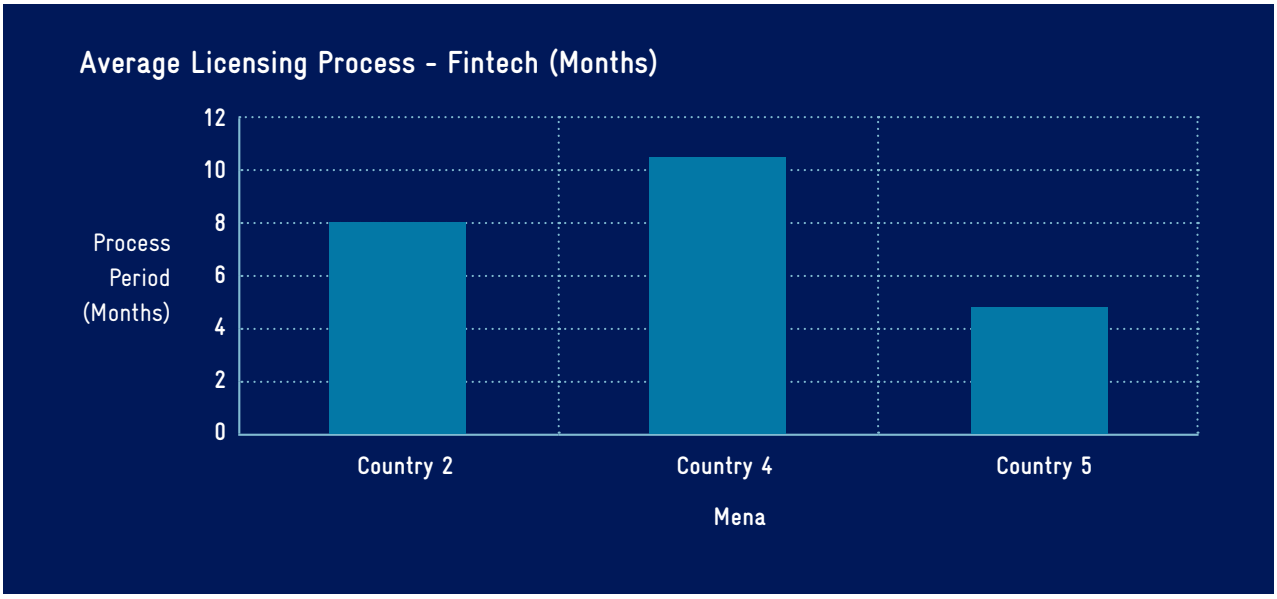
Sample: 6 countries
Total in the sample:
3 Sandboxes (2 active and 1 proposed)
4 Innovation Hubs (2 active and 2 proposed)

Average licensing process (months) for banks: 9.7 months
Average licensing process (months) for Non-Banks: 7 months
Average licensing process (months) for Fintechs: 7.8 months





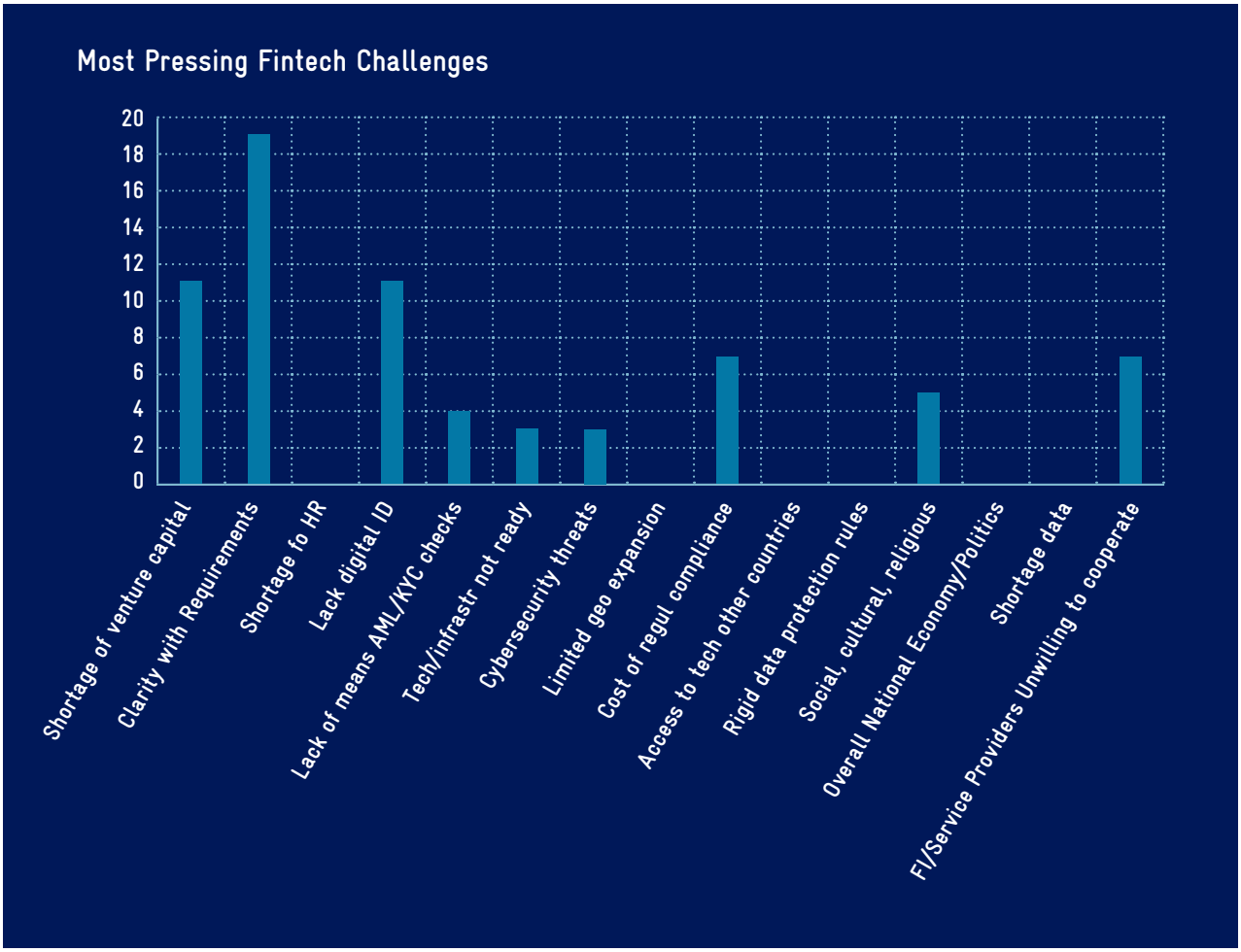




The chart below shows the top Fintech Challenges in the region (score built as sum of the scores collected from all respondents: most pressing challenge=5, least pressing challenge=1). The score shows a value of importance per challenge in the MENA region. The higher the score, the more pressing is a specific challenge in the region.

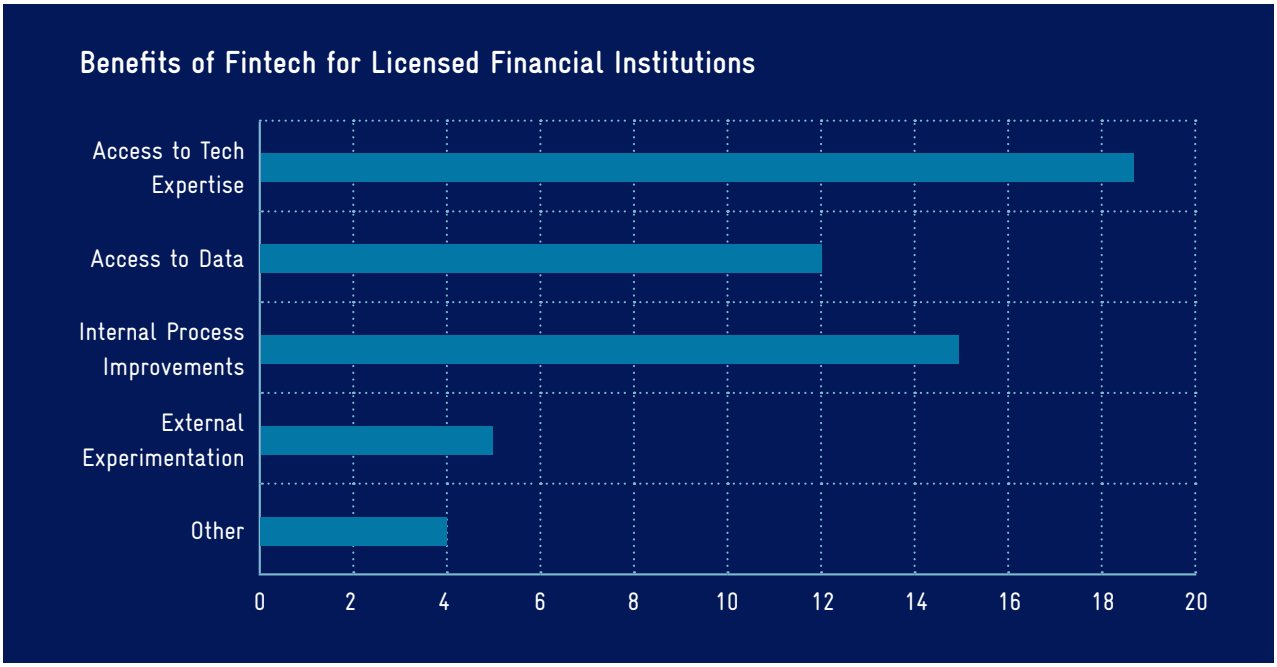
Top 5 most pressing Fintech challenges in the MENA region:

1 Clarity with regulatory and licensing requirements
2 Lack of means for digital identification and onboarding of clients
3 Cost of regulatory compliance
4 Established financial institutions or service providers unwilling to cooperate (same scoring as '3-Cost of regulatory compliance')
5 Social, cultural, religious

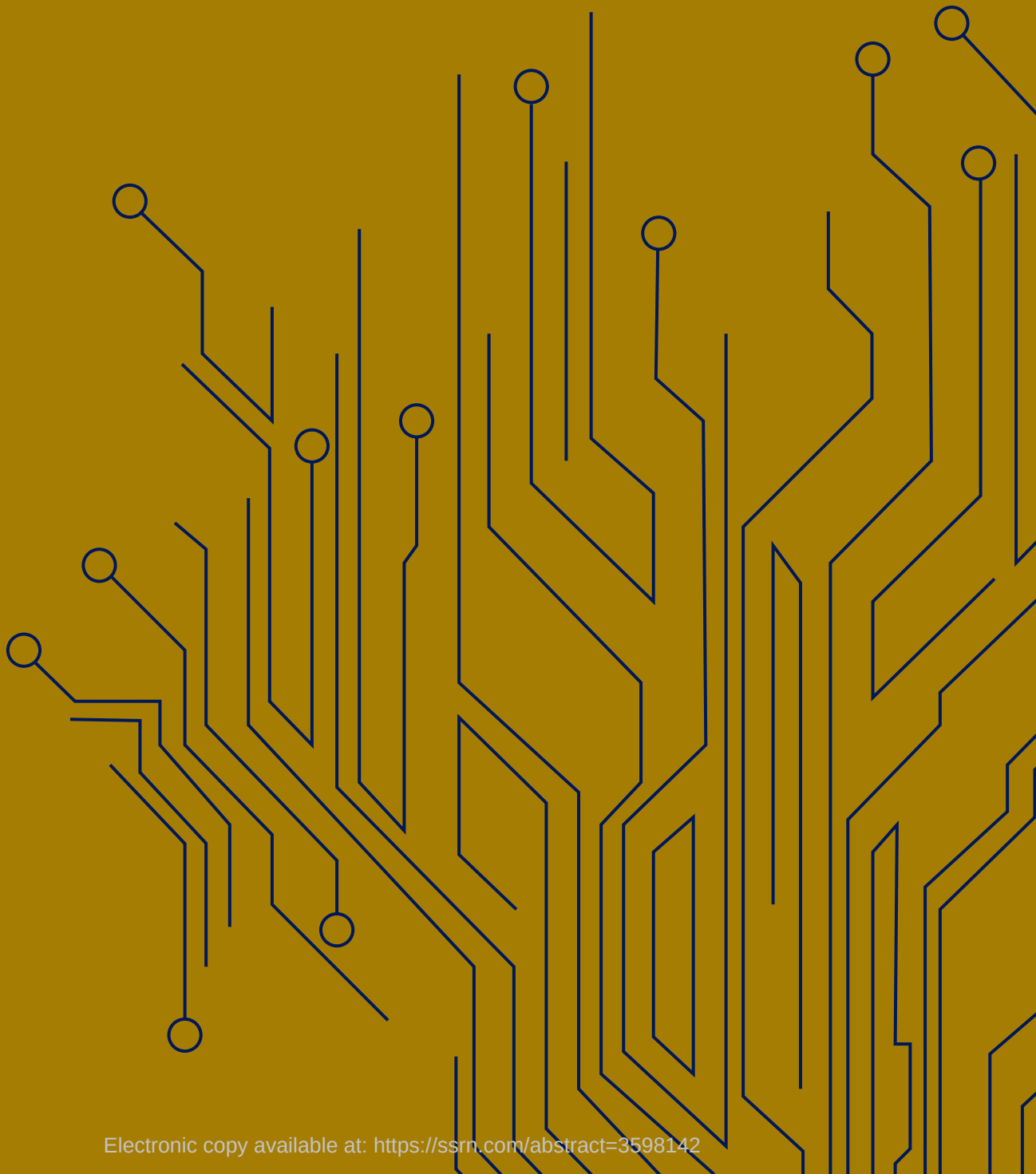


The chart below shows the most important benefits of Fintech for licensed financial institutions (score built as sum of the scores collected from all respondents: most important benefit=5, least important benefit=1).

MENA countries consider Fintechs beneficial for licensed financial institutions because they ease their access to tech expertise.



ANNEX 3:
USEFUL RESOURCES



Fintech: Taxonomy and Framework

AI and Machine Learning: Suggested Resources

Regulatory Bodies and NGOs

- **BaFin,** 'Big data meets artificial intelligence Challenges and implications for the supervision and regulation of financial services' (July 2018) *https://www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.pdf?__blob=publicationFile&v=11*
- **Bauguess, Scott W.,** 'The Role of Big Data, Machine Learning, and AI in Assessing Risks: a Regulatory Perspective' (21 June 2017) Acting Director and Acting Chief Economist, DERA, Champagne Keynote Address New York *https://www.sec.gov/news/speech/bauguess-big-data-ai*
- **Baugness, Scott W.,** 'The Role of Machine Readability in an AI World' (3 May 2018) Deputy Chief Economist and Deputy Director, Division of Economic and Risk Analysis, SEC Keynote Address: Financial Information Management (FIMA) Conference 2018, Boston, Massachusetts, *https://www.sec.gov/news/speech/speech-bauguess-050318*
- **BIS,** *The use of big data analytics and artificial intelligence in central banking* (May 2019) BISIFC Bulletin No 50.
- **Brainard, Lael,** What Are We Learning about Artificial Intelligence in Financial Services? (13 November 2018) Board of Governors of the Federal Reserve System at Fintech and the New Financial Landscape, Hosted by the Federal Reserve Bank of Philadelphia, The Federal Deposit Corporation, University of Pennsylvania Wharton School of Business, Bank Policy Institutem and Brookings Institution, Philadelphia, Pennsylvania.
- **Carney, Mark,** Enable, Empower, Ensure: A New Finance for the New Economy (20 June 2019) Bank of England, Speech at the Lord Mayor's Banquet for Bankers and Merchants of the City of London at Mansion House, London.
- **Cantu, Carlos, Stijn Claessens and Leonardo Gamgacorto,** How do bank-specific characterisitcs affect lending? New evidence based on credit registry data from Latin America (July 2019) BIS Working Paper No 798.
- **De Nederlandsche Bank (Dutch Central Bank),** General principles for the use of Artificial Intelligence in the financial sector (2019), *https://www.dnb.nl/binaries/General%20principles%20for%20the%20use%20of%20Artificial%20Intelligence%20in%20the%20financial%20sector_tcm46-385055.pdf*
- **European Commission,** Fintech Action Plan (March 2018), *https://ec.europa.eu/info/publications/180308-action-plan-fintech_en*
- **European Securities and Markets Authority,** 'ESMA response to the Commission Consultation Paper on Fintech: A More competitive and innovative financial sector' (7 June 2017) *https://www.esma.europa.eu/press-news/esma-news/esma-responds-commission-consultation-fintech*
- **Falk, Magnus,** 'Artificial Intelligence in the boardroom' (01 August 2019) FCA Insight, *https://www.fca.org.uk/insight/artificial-intelligence-boardroom*
- **Financial Stability Board,** 'Artificial intelligence and machine learning in financial services - Market developments and financial stability implications' (1 November 2017) *https://www.fsb.org/wp-content/uploads/P011117.pdf*
- **Grupetta, Rob,** 'Using artificial intelligence to keep criminal funds out of the financial system' Head of the Financial Crime Department at the FCA, delivered to the Fintech Innovation in AML and Digital ID regional event, London (06 December 2017) *https://www.fca.org.uk/news/speeches/using-artificial-intelligence-keep-criminal-funds-out-financial-system*
- **Hong Kong Monetary Authority,** High-level Principles on Artificial Intelligence, 1 November 2019, *https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191101e1.pdf*
- **Hunt, Stefan,** 'From Maps to Apps: the Power of Machine Learning and Artificial Intelligence for Regulators' Head of Behavioural Economics and Data Science, Financial Conduct Authority, Speech at Beesley Lecture Series on regulatory economics (19 October 2017) *https://fca.org.uk/publication/documents/from-maps-to-apps.pdf*
- **Kuroda, Haruhiko,** *AI and the Frontiers of Finance,* (13 April 2017) Bank of Japan, Conference on "AI and Financial Services/Financial Markets", Tokyo
- **Lagarde, Christine,** '*Central Banking and Fintech – A Brave New World?'* (29 September 2017) IMF Managing Director Bank of England conference, London
- **Greg Medcraft,** 'Driving better consumer outcomes in the era of big data and artificial intelligence' ASIC Chairman Corporate Governance Discussion Group Sydney, Australia (3 November 2016) *https://download.asic.gov.au/media/4064271/greg-medcraft-speech-corp-governance-discussion-group-published-3-november-2016.pdf*
- **Monetary Authority of Singapore,** 'Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector' (November 2018) *https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf*
- **OECD,** *OECD Principles on AI,* (22 May 2019)

- **OECD Council,** *Recommendation of the Council on Artificial Intelligence* (22 May 2019)
- **G20,** *G20 Ministerial Statement on Trade and Digital Economy,* (9 June 2019)
- **OECD,** *Artificial Intelligence in Society* (11 June 2019)
- **OECD (2018),** "Private Equity Investment in Artificial Intelligence", OECD Going Digital Policy Note, OECD, Paris, *www.oecd.org/going-digital/ai/private-equity-investment-in-artificial-intelligence.pdf*
- **OECD (October 2017)** "AI: Intelligent machines, smart policies", OECD Digital Economy Papers, OECD, Paris, *https://www.oecd-ilibrary.org/docserver/f1a650d9-en.pdf?expires=1567911008&id=id&accname=guest&checksum=-61C249A082F002B8107EBC4664AC1DAF*
- **OECD (October 2017)** "Technology Outlook: artificial intelligence and blockchain" in OECD Digital Economy Outlook 2017, OECD, Paris, *https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2017/technology-outlook_9789264276284-10-en*
- **OECD (19 November 2018)** 'Artificial intelligence and machine learning in science' and Artificial intelligence and the technologies of the next production revolution' in OECD Science, Technology and Innovation Outlook, OECD, Paris, *https://www.oecd.org/sti/oecd-science-technology-and-innovation-outlook-25186167.htm*
- **Proudman, James,** *Managing machines - the governance of artificial intelligence* (4 June 2019) Executive Director of UK Deposit Takers Supervision of the Bank of England, at the FCA Conference on Governance in Banking, London
- **Panetta, Fabio, Harnessing** Big Data & Machine Learning Technologies for Central Banks (26 March 2018) Banca D'Italia.
- **James Proudman,** 'Cyborg supervision – the application of advanced analytics in prudential supervision' Executive Director, UK Deposit Takers, Speech given at workshop on research on bank supervision, Bank of England (19 November 2018) *https://www.bankofengland.co.uk/speech/2018/james-proudman-cyborg-supervision*
- **Wuermeling, Joachim**, Artifical intelligence (AI) in finance – six warnings from a central banker (27 Feb 2018) BIS.
- **World Economic Forum,** The New Physics of Financial Services - Understanding how artificial intelligence is transforming the financial ecosystem (Aug 2018), *http://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf*

Private Entities

- From Principles to Practice – Use Cases for Implementing Responsible AI in Financial Services (Nov. 2019), *https://www.microsoft.com/cms/api/am/binary/RE487kh*
- **UK Finance,** Artificial Intelligence in Financial Services (Jun. 2019), *https://www.ukfinance.org.uk/system/files/AI-2019_FINAL_ONLINE.pdf*

Academic Literature

- **Borselli, Angelo,** Insurance by Algorithm. European Insurance Law Review, No. 2, 2018; Bocconi Legal Studies Research Paper No. 3284437. Available at SSRN: *https://ssrn.com/abstract=3284437*
- **Casey, Anthony J. & Niblett,** Anthony, The Death of Rules and Standards, 92 Ind. L.J. 1401, 1410-12 (2017) (arguing that technology will facilitate the emergence of individualized micro-directives in between rules and standards);
- **Casey, Anthony J. & Niblett, Anthony,** Self-driving contracts, 43 J. Corp. L. 1, 13-26 (2017) (arguing that technology will lead to subject-specific, self-completing contract law);
- **Casey, Anthony J. & Niblett, Anthony,** A Framework for the New Personalization of Law, U. Chi. L. Rev. (forthcoming 2019) (developing preconditions for AI-based reconfiguration of the law);
- **Davis, Joshua P.,** Laws without Mind: AI, Ethics, and Jurisprudence (Fall 2018) 55 California Western Law Review 1, pp. 165-220.
- **Enriques, Luca & Zetzsche, Dirk A.,** Corporate Technologies and the Tech Nirvana Fallacy, European Corporate Governance Institute (ECGI) - Law Working Paper No. 457/2019, *https://ssrn.com/abstract=3392321*
- **Etzioni, Amitai, & Oren Etzioni,** Keeping AI Legal (Fall 2016) 19 Vanderbilt Journal of Entertainment and Technology 1, pp. 133-146.
- **Fenwick, Mark & Vermeulen, Erik P.M.,** Technology and Corporate Governance: Blockchain, Crypto, and Artificial Intelligence (October 9, 2018). European Corporate Governance Institute (ECGI) – Law Working Paper No. 424/2018. Available at SSRN: *https://ssrn.com/abstract=3263222* or *http://dx.doi.org/10.2139/ssrn.3263222*
- **Jackson, Brandon W.,** Artificial Intelligence and The Fog of Innovation: A Deep-dive on Governance and the Liability of Autonomous Systems (2019) 35 Santa Clara High Technology Law Journal 4.
- **Katz, Daniel M.,** Quantitative Legal Prediction – or How I Learned to Stop Worrying and Start Preparing for the Data Driven Future of the Legal Services Industry, 62 Emory L.J. 909 (2013) (highlighting the opportunities of data-driven quantitative predictions for the legal profession);
- **Lin, Tom C. W.,** The New Investor. 60 UCLA Law Review 678 (2013); 60 UCLA Law Review 678 (2013)

- **Marano, Pierpaolo,** Navigating InsurTech: The digital intermediaries of insurance products and customer protection in the EU (2019) Maastricht Journal of European and Comparative Law 1-22.
- **McPhail, Lihong and McPhail, Joseph,** Machine Learning Implications for Banking Regulation (July 20, 2019). Available at SSRN: *https://ssrn.com/abstract=3423413 or http://dx.doi.org/10.2139/ssrn.3423413*
- **Scherer, Matthew U.,** Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies (Spring 2016) 29 Harvard Journal of Law & Technology 2.
- **Scott, Kate,** AI and Risk for Financial Institutions (2019) International Financial Law Review 110.
- **Surden, Harry,** Machine Learning and Law, 89 U. Wash. L. Rev. 87,102–10 (2014) (discussing progress on AI research and how it may affect the practice of the law).
- **Zetzsche, Dirk A., Arner, Douglas W., Buckley, Ross P. and Tang, Brian,** Artificial Intelligence, Fintech and Regtech, Working Paper (Dec. 2019). *www.ssrn.com/abstract=3531711*

Big Data: Suggested Resources

Regulatory Bodies and NGOs

- **Awara, Luiz, Pereira da Zilva and Goetz von Peter,** Financial instability: can Big Data help connect the dots? (29 November 2018) BIS, Remarks, Ninth European Central Bank Statistics Conference, Frankfurt.
- **BaFin,** 'Big data meets artificial intelligence Challenges and implications for the supervision and regulation of financial services' (July 2018) *https://www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.pdf?__blob=publicationFile&v=11*
- **Bailey, Andrew,** 'The challenges for insurance and regulators in a Big Data world' Chief Executive of the FCA, speech delivered at the Association Of British Insurers (ABI) annual conference (22 November 2016) *https://www.fca.org.uk/news/speeches/challenges-insurance-regulators-big-data-world*
- **Bauguess, Scott W.,** 'The Role of Big Data, Machine Learning, and AI in Assessing Risks: a Regulatory Perspective' (21 June 2017) Acting Director and Acting Chief Economist, DERA, Champagne Keynote Address New York *https://www.sec.gov/news/speech/bauguess-big-data-ai*
- **Bauguess, Scott W.,** 'Has Big Data Made Us Lazy?' (21 October 2016) Deputy Director and Deputy Chief Economist, DERA, Midwest Region Meeting – American Accounting Association (AAA), Chicago Illinois *https://www.sec.gov/news/speech/bauguess-american-accounting-association-102116.html*
- **Bholat, David,** 'Big data and central banks' Bank of England Quarterly bulleting 2015 Q1 (9 March 2015) *https://www.bankofengland.co.uk/quarterly-bulletin/2015/q1/big-data-and-central-banks*
- **BIS,** 'Central banks' use of and interest in "big data"' (October 2015) BIS IFC Report *https://www.bis.org/ifc/publ/ifc-report-bigdata.pdf*
- **BIS,** Big Data (16 September 2017) BIS IFC Bulleting No. 44 *https://www.bis.org/ifc/publ/ifcb44.htm*
- **BIS,** The use of big data analytics and artificial intelligence in central banking (May 2019) BIS IFC Bulletin No 50.
- **BIS,** 'Building Pathways for Policy Making with Big Data' BI-IFC/BIS International Seminar on Big Data (26 July 2018) Bank of Indonesia and Irving Fisher Committee on Central Bank Statistics BIS *https://www.bis.org/ifc/events/big_data_jul_18/ifc_big_data_jul_18_seminar.pdf*
- **BIS,** Are post-crisis statistical initiatives completed? (January 2019) BIS IFC Bulletin No 49.
- **Buch, Claudia,** Digitalization, competition, and financial stability (17 August 2019) Opening remarks, Seminar – Statistics on Fintech – Bring Together Demand and Supply to Measure its Impact, Kuala Lumpur.
- **Cantu, Carlos, Stijn Claessens and Leonardo Gambacorto,** How do bank-specific characterisitcs affect lending? New evidence based on credit registry data from Latin America (July 2019) BIS Working Paper No 798.
- **Coeure, Benoit,** 'Policy analysis with big data' Member of the Executive Board of the European Central Bank, at the conference on "Economic and Financial Regulation in the Era of Big Data", organised by the Bank of France, Paris (24 November 2017) *https://www.bis.org/review/r171124c.pdf*
- **FCA,** 'Feedback Statement: Cal for Inputs on Big Data in retail general insurance" (September 2016) *https://www.fca.org.uk/publication/feedback/fs16-05.pdf*
- Galhau, Francois Villeroy de, 'Economic and financial regulation in the era of big data' Governor of the Bank of France, at the Conference on "Economic and Financial Regulation in the Era of Big Data", Paris, (24 November 2017) *https://www.bis.org/review/r171229h.pdf*
- **GIZ,** Responsible Use of Personal Data and Automated Decision-making in Financial Services (Aug. 2018) *https://responsiblefinanceforum.org/wp-content/uploads/2018/10/2018-08-22-Reponsible-use-of-personal-data-and-automated-decision-making-in-financial-services.pdf*
- **Joint Committee of the European Supervisory Authorities,** 'Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions' (July 2016) *https://www.esma.europa.eu/system/files_force/library/jc-2016-86_discussion_paper_big_data.pdf?download=1*

- **Kothari, S.P.,** 'Policy Challenges and research Opportunities in the Era of Big Data' (13 July 2019) Chief Economist and Director, Division of Economic and Risk Analysis, Big Data and High-Performance Computing for Financial Economics, National Bureau of Economic Research, Cambridge, MA *https://www.sec.gov/news/speech/policy-challenges-research-opportunities-era-big-data*
- **Nymand-Andersen, Per, Emmanouil Pantelidis,** 'Google econometrics: nowcasting euro area car sales and big data quality requirements' European Central Bank Statistics Paper series (November 2018) *https://www.ecb.europa.eu/pub/pdf/scpsps/ecb.sps30.en.pdf?eedf0180991148966fdff1e9fe872a9b*
- **OECD,** 'Data driven innovation for growth and well being' (6 October 2015) *https://read.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en#page1*
- **OECD,** 'Big Data: Bringing competition policy to the digital era' (26 April 2017) *https://one.oecd.org/document/DAF/COMP/M(2016)2/ANN4/FINAL/en/pdf*
- **Panetta, Fabio,** Harnessing Big Data & Machine Learning Technologies for Central Banks (26 March 2018) Banca D'Italia.
- **Rossi, Salvatore,** 'Big Data econometrics with applications' Senior Deputy Governor of the Bank of Italy and President of the Institute for the Supervision of Insurance (IVASS), at the 29th (EC)2 Conference on "Big Data Econometrics with Applications", Rome, (13 December 2018) *https://www.bis.org/review/r181213c.pdf*
- **Signorini, Luigi Federico,** 'Harnessing big data & machine learning technologies for central banks' Deputy Governor of the Bank of Italy, at the workshop on "Harnessing Big Data & Machine Learning Technologies for Central Banks", Bank of Italy (10 April 2018) *https://www.bis.org/review/r180410b.pdf*
- **Sinha, Nitish,** 'Using big data in finance: Example of sentiment-extraction from news articles' FEDS Notes (26 March 2014) *https://www.federalreserve.gov/econresdata/notes/feds-notes/2014/using-big-data-in-finance-example-of-sentiment-extraction-from-news-articles-20140326.html*
- **Stein, Kara M.,** 'A Vision for Data at the SEC' (28 October 2016) Commissioner of the SEC, Keynote address to Big Data in Finance Conference *https://www.sec.gov/news/speech/speech-stein-10-28-2016.html*
- **Stein, Kara M.,** 'From the Data Rush to the Data Wars: A Data Revolution in Financial Markets' (28 October 2016) Commissioner of the SEC, (27 September 2018) Georgia State University College of Law – Henry J. Miller Distinguished Lecture Series *https://www.sec.gov/news/speech/speech-stein-092718*
- **Thorsrud, Leif Anders,** 'Nowcasting using news topics Big Data versus big bank' European Central bank Working Paper (21 December 2016) *https://www.ecb.europa.eu/pub/conferences/shared/pdf/20170929_advances_in_short_term_forecasting/Paper_5_Thorsrud.pdf*
- **Tissot, Bruno,** 'Big data and central banking' IFc Bulletin 44 (21 September 2017) *https://www.bis.org/ifc/publ/ifcb44_overview_rh.pdf*
- **UNCDF,** 'Big data4What?' (18 December 2018) *https://www.uncdf.org/article/4216/bigdata4what*

Academic Literature

- **Arner, Douglas W., Barberis, Janos Nathan & Buckley, Ross P.,** The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data, (2016) 44 Journal of Financial Transformation 79; UNSW Law Research Paper No. 17-63. Available at SSRN: *https://ssrn.com/abstract=3044280*
- **Arner, Douglas W., Zetzsche, Dirk A., Buckley, Ross P. & Barberis, Janos Nathan,** Fintech and Regtech: Enabling Innovation While Preserving Financial Stability, (2017) 18(3) Georgetown Journal of International Affairs 47.
- **Barocas, Solon, & Andrew D. Selbst,** Big Data's Disparate Impact 104 Cal. L. Rev. 671 (2016) (highlighting data dependency and the risk that algorithms simply reflect existing biases in society);
- **Cohen, Julie E.,** What Privacy Is For, 126 Harv. L. Rev. 1904, 1918 (2013) (arguing that big data is an euphemism that conceals efforts to repackage pervasive surveillance as innovation and asking to balance data processing and privacy priorities);
- **Elvy, Stacy-Ann,** Paying for Privacy and the Personal Data Economy, 117 Colum. L. Rev. 1369, 1400-28 (2017) (developing a typology of data business models and highlighting similarities and tensions between a commercial data market and consumers' privacy interests);
- **Kuhn, Mckenzie L.,** 147 Million Social Security Numbers for Sale: Developing Data Protection Legislation After Mass Cybersecurity Breaches, 104 Iowa L. Rev. 417, 421-435 (2018) (arguing in favor of adopting federal data protections laws);
- **Scott, Kate,** AI and Risk for Financial Institutions (2019) International Financial Law Review 110.
- **Zetzsche, Dirk A., Ross P. Buckley, Douglas W. Arner & Janos N. Barberis,** From Fintech to Techfin: The Regulatory Challenges of Data-Driven Finance, 14 N.Y.U. J.L. & Bus. 393, 435-443 (2018) (arguing in favor of data-specific adjustments to financial regulations). Available at SSRN: *https://ssrn.com/abstract=2959925*

- **Zetzsche, Dirk A., Arner, Douglas W., Buckley, Ross P. & Weber, Rolf H.,** The Future of Data-Driven Finance and Regtech: Lessons from EU Big Bang II, European Banking Institute Working Paper Series 2019/35. Available at SSRN: *https://ssrn.com/abstract=3359399 or http://dx.doi.org/10.2139/ssrn.3359399*
- **Zetzsche, Dirk A., Buckley, Ross P. & Arner, Douglas W.,** Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses. Available at SSRN: *https://ssrn.com/abstract=3414401*

Cloud Solutions: Suggested Resources

Regulatory Bodies and NGOs

- **APRA,** 'Information Paper Outsourcing Involving Cloud Computing Services' (24 September 2018) *https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf*
- **Bank of England,** 'New economy, new finance, new bank: The Bank of England's response to the can Steenis review on the future of Finance' (June 2019) *https://www.bankofengland.co.uk/-/media/boe/files/report/2019/response-to-the-future-of-finance-report.pdf?la=en&hash=C4FA7E3D277DC82934050840DBCFBFC7C67509A4#page=11*
- **Basel Committee on Banking Supervision,** 'Sound Practices: Implications of fintech developments for banks and bank supervisors' (February 2018) *https://www.bis.org/bcbs/publ/d431.pdf*
- **Brainard, Lael,** 'Where Do Consumers Fit in the Fintech Stack?' "Fintech Risks and Opportunities: An Interdisciplinary Approach," a conference sponsored by the University of Michigan, Ann Arbor, Michigan (16 November 2017) *https://www.federalreserve.gov/newsevents/speech/brainard20171116a.htm*
- **David Byrne, Carol Corrado, Daniel Sichel,** 'The Rise of Cloud Computing: Minding Your P's, Q's and K's' Working Paper for the 5th IMF Statistical Forum: Measuring the Digital Economy (March 2017) *https://www.imf.org/~/media/Files/Conferences/2017-stats-forum/david-byrne-11-17-presentation.ashx*
- **Carney, Mark,** Enable, Empower, Ensure: A New Finance for the New Economy (20 June 2019) Bank of England, Speech at the Lord Mayor's Banquet for Bankers and Merchants of the City of London at Mansion House, London.
- **CSISAC,** 'Cloud Computing: The Next Computing Paradigm?' CSISAC comments on Cloud Computing: Portability, Competition, Innovation *https://www.oecd.org/sti/ieconomy/43922341.pdf*
- **Financial Stability Board,** 'Fintech and market structure in financial services: Market developments and potential financial stability implications' (14 February 2019) *https://www.fsb.org/wp-content/uploads/P140219.pdf*
- **Financial Stability Institute,** 'Regulating and Supervising the Clouds', FSI Insights No 13 (December 2018) *https://www.bis.org/fsi/publ/insights13.pdf*
- **Financial Stability Board,** 'Decentralized financial technologies – Report on financial stability, regulatory and governance implications' (6 June 2019) *https://www.fsb.org/wp-content/uploads/P060619.pdf*
- *Financial Stability Board,* 'Crypto-asset markets – Potential channels for future stability implications' (10 October 2018) *https://www.fsb.org/wp-content/uploads/P101018.pdf*
- **Joint committee of the European Supervisory Authorities,** 'Joint Committee Report on Risks and Vulnerabilities in the EU Financial System' (April 2018) *https://esas-joint-committee.europa.eu/Publications/Reports/Joint%20Committee%20Risk%20Report.pdf*
- **Mattern, Mac,** 'Exploring Blockchain applications to Agricultural Finance' (July 2018) *https://www.cgap.org/sites/default/files/researches/documents/Brief-Exploring-Blockchain-Applications-July-2018.pdf*
- **OECD,** 'Cloud Computing: The Concept, Impacts and the Role of Government Policy' (19 August 2014) *https://www.oecd-ilibrary.org/docserver/5jxzf4lcc7f5-en.pdf?expires=1567934928&id=id&accname=guest&checksum=56F8F59B2C49392FC6FE575F27794742*
- **OECD,** 'Cloud Computing and Public Policy' Briefing Paper for the ICCP Technology Foresight Forum (14 October 2009) *https://www.oecd.org/sti/ieconomy/43933771.pdf*
- **UNCDF,** 'Demystifying blockchain and its uses for international development' (18-20 June 2018) *https://www.uncdf.org/article/3982/*

Academic Literature

- **Buckley, Ross P., Arner, Douglas W., Zetzsche, Dirk A. and Selga, Eriks,** 'The Dark Side of Digital Financial Transformation: The New Risks of Fintech and the Rise of TechRisk'. Available at: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478640*

Distributed Ledgers and Blockchain

Regulatory Bodies and NGO

- **Ali, Robleh, John Barrdear, Roger Clews and James Southgate,** 'Innovations in payment technologies and the mergence of digital currencies' Bank of England Quarterly Bulletin 2014 Q3 (16 September 2014) *https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2014/innovations-in-payment-technologies-and-the-emergence-of-digital-currencies.pdf?la=en&hash=AB46869B3EF355A0486F7B0BAF086F2EEE31554D*
- **Awazu, Luiz and Pereira da Silva,** Fintech in EMEs: blessing or curse? (5 June 2018) BIS, Panel remarks at CV Meeting of Central Bank Governors of CEMLA – Asuncion, Paraguay.
- **ASIC,** 'Evaluating distributed ledger technology' ASIC Information sheet 219 *https://asic.gov.au/regulatory-resources/digital-transformation/evaluating-distributed-ledger-technology/*
- **Athanassiou, Phoebus,** 'Impact of digital innovation on the processing of electronic payments and contracting: an overview of legal risks' European Central Bank Legal Working Paper Series No 16 (October 2017)
- **Bajwa, Tariq,** 'International remittance through blockchain technology launch' Governor of the State Bank of Pakistan, at the launching ceremony of international remittance through block chain technology, Islamabad (8 January 2019) *https://www.bis.org/review/r190115b.pdf*
- **Barrdear, John, and Micheal Kumhof,** 'The Macroeconomics of central bank issued digital currencies' Bank of England Working Paper No. 605 (18 July 2016) *https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies.pdf?la=en&hash=341B602838707E5D6FC26884588C912A721B1DC1*
- **Benos, Evangelos, Rodney Garratt and Pedro Gurrola-Perez,** 'The economics of distributed ledger technology for securities settlement' Bank of England Working Paper 670 (18 August 2017) *https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2017/the-economics-of-distributed-ledger-technology-for-securities-settlement.pdf?la=en&hash=17895E1C1FEC86D37E12E4BE63BA9D9741577FE5*
- **BIS,** Committee on Payments and Market Infrastructures, 'Distributed ledger technology in payment, clearing and settlement – an analytical framework' CPMI Papers No 157 (27 February 2017) *https://www.bis.org/cpmi/publ/d157.pdf*
- **Brainard, Lael,** 'Cryptocurrencies, digital currencies, and distributed ledger technologies – what are we learning?' Member of the Board of Governors of the Federal Reserve System, at the Decoding Digital Currency Conference, sponsored by the Federal Reserve Bank of San Francisco, San Francisco, California (15 May 2018) *https://www.bis.org/review/r180516d.pdf*
- **Carstens, Agustin,** Money in a digital age: 10 thoughts (15 November 2018) BIS, Singapore, Speech.
- **Cermano, Javier Sebastian,** 'Blockchain in financial services: Regulatory landscape and future challenges for its commercial application' 16/20 Working Paper BBVA research (December 2016) *https://www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf*
- **ECB,** STELLA – a joint research project of the European Central Bank and the Bank of Japan 'Securities settlement systems: delivery-versus-payment in a distributed ledger environment' (March 2018) *https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf*
- **ECB,** STELLA – a joint research project of the European Central Bank and the Bank of Japan, 'Payment systems: liquidity saving mechanisms in a distributed ledger environment' (September 2017) *https://www.ecb.europa.eu/pub/pdf/other/ecb.stella_project_report_september_2017.pdf*
- **ESMA,** 'The Distributed Ledger Technology Applied to Securities Markets' (7 February 2017) *https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf*
- **Financial Conduct Authority,** 'Distributed Ledger Technology – Feedback Statement on Discussion Paper 17/03' (December 2017) *https://www.fca.org.uk/publication/feedback/fs17-04.pdf*
- **Financial Conduct Authority,** 'Discussion Paper on distributed ledger technology' (April 2017) *https://www.iosco.org/library/ico-statements/United%20Kingdom%20-%20FCA%20-%20Discussion%20Paper%20on%20distributed%20ledger%20technology.pdf*
- **Googoolye, Yandraduth,** 'Blockchain technology's potential to benefit society and the economy' Governor of the Bank of Mauritius, Prelude to Banquet in the context of the ADC Global Blockchain Summit, Adelaide (27 March 2019) *https://www.bis.org/review/r190329g.pdf*
- **Institute of International Finance,** 'Improving global AML efforts with technology and regulatory reform' (29 November 2017) *https://www.iif.com/portals/0/Files/private/32370132_iif_-_aml_regtech_and_reg_reform_nov_2017.pdf*
- **International Finance Corporation,** 'Blockchain – Opportunities for Private Enterprises in Emerging Markets' (January 2019) *https://www.ifc.org/wps/wcm/connect/2106d1c6-5361-41cd-86c2-f7d16c510e9f/201901-IFC-EMCompass-Blockchain-Report.pdf?MOD=AJPERES&CVID=mxYj-sA*

- **IOSCO,** 'IOSCO Research Report on Financial Technologies (Fintech)' (February 2017) *https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf*
- **Knot, Klass,** 'The evolution of power of blockchain – a central banker's balancing act' President of the Netherlands Bank, at the EBF Conference "The Evolution of Power", Groningen (5 October 2018) *https://www.bis.org/review/r181015j.pdf*
- **Linneman Bech, Morten and Rodney Garratt,** 'Central Bank Cryptocurrencies' BIS Quarterly Review (17 September 2017) *https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf*
- **Maechler, Andre M.,** The financial markets in changing times Changes today and tomorrow: the digital future (5 April 2018) Bank of Switzerland, Money Market Event, Speech.
- **Menon, Ravi,** 'Economic possibilities of blockchain technology' Managing Director of the Monetary Authority of Singapore, at the Global Blockchain Business Conference, Singapore (9 October 2017) *https://www.bis.org/review/r171010b.pdf*
- **Mersch, Yves,** 'Distributed ledger technology – panacea or flash in the pan?' Member of the Executive Board of the European Central Bank, at the Deutsche Bank Transaction Bankers' Forum 2016, Frankfurt am Main (25 April 2016) *https://www.bis.org/review/r160426b.pdf*
- **Mersch, Yves,** 'Distributed ledger technology – role and relevance of the European Central Bank' Member of the Executive Board of the European Central Bank, at the 22nd Handelsblatt Annual Conference "Banken-Technologie", Frankfurt am Main (6 December 2016) *https://www.bis.org/review/r161212c.pdf*
- **OECD,** 'Blockchain and distributed ledger technology' *http://www.oecd.org/daf/blockchain/*
- **Pinna, Andrea, and Wiebe Ruttenberg,** 'Distributed ledger technologies in securities post-trading – Revolution or evolution?' European Central Bank Occasional Paper Series No 172 (April 2016) *https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf*
- **Starks, Mary,** 'Blockchain: considering the risks to consumers and competition' Director of Competition, FCA, at Authority for Consumers & Markets Conference Panel, Netherlands (26 April 2018) *https://www.fca.org.uk/news/speeches/blockchain-considering-risks-consumers-and-competition*
- **Starks, Mary,** 'Disruptive innovation in financial markets' Director of Competition, FCA, delivered at the OECD (Organisation for Economic Cooperation and Development), Paris (26 October 2015) *https://www.fca.org.uk/news/speeches/disruptive-innovation-financial-markets*
- **Tapscott, Don, and Alex Tapscott** 'Realizing the Potential of Blockchain – A Multistakeholder Approach to the Stewardship of blockchain and Cryptocurrencies' World Economic Forum White Paper (June 2017) *http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf*
- **Thiele, Carl-Ludwig,** 'Blockchain technology – opportunities and challenges' Member of the Executive Board of the Deutsche Bundesbank, at the 6th Central Banking Workshop 2016, Eltville, (21 November 2016) *https://www.bis.org/review/r161125b.pdf*
- **Thiele, Carl-Ludwig,** 'Industry Dialogue on "Distributed ledger technology – potential benefits and risks" Member of the Executive Board of the Deutsche Bundesbank, at the G20 conference "Digitising finance, financial inclusion and financial literacy", Wiesbaden (26 January 2017) *https://www.bis.org/review/r170131e.pdf*
- **Christopher Woolard,** Conclusions from the Cyrptoassets Taskforce' Executive Director of Strategy and Competition at the FCA, delivered at The Regulation of Cryptocurrencies event, London (20 November 2018) *https://www.fca.org.uk/news/speeches/conclusions-cryptoassets-taskforce*

Academic Literature

DLT and Digital Assets

- **Arner, Douglas W., Buckley, Ross P., Didenko, Anton, Park, Cyn-Young, Pashoska, Emilija, Zetzsche, Dirk A. and Zhao, Bo,** Distributed Ledger Technology and Digital Assets – Policy and Regulatory Challenges in Asia, Asian Development Bank Economics Working Paper Series. Available at SSRN: *https://ssrn.com/abstract=3414408*
- **Chohan, Usman W.,** Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability (November 30, 2017). Available at SSRN: *https://ssrn.com/abstract=3080098 or http://dx.doi.org/10.2139/ssrn.3080098*
- **Donald, David C. and Miraz, Mahdi H.,** Multilateral Transparency for Securities Markets through DLT (July 26, 2019). The Chinese University of Hong Kong Faculty of Law Research Paper No. 2019 - 05. Available at SSRN: *https://ssrn.com/abstract=3352293*
- **Kaal, Wulf A.,** Initial Coin Offerings: The Top 25 Jurisdictions and Their Comparative Regulatory Responses (February 2, 2018). CodeX Stanford Journal of Blockchain Law & Policy (2018); U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-07. Available at SSRN: *https://ssrn.com/abstract=3117224 or http://dx.doi.org/10.2139/ssrn.3117224*
- **Perlman, Leon,** A Model Crypto-Asset Regulatory Framework (May 16, 2019). Available at SSRN: *https://ssrn.com/abstract=3370679* or *http://dx.doi.org/10.2139/ssrn.3370679*

- **Zetzsche, Dirk Andreas, Ross P. Buckley and Douglas W. Arner,** The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain, 2018 U. Ill. L. Rev. 1361, 1382-1402.
- **Zetzsche, Dirk Andreas, Buckley, Ross P., Arner, Douglas W. and Föhr, Linus,** The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators; 60:2 Harvard International Law Journal 321 (2019). Available at SSRN: *https://ssrn.com/abstract=3072298 or http://dx.doi.org/10.2139/ssrn.3072298*

Blockchain

- **Finck, Michèle,** Blockchains and Data Protection in the European Union (November 30, 2017). Max Planck Institute for Innovation & Competition Research Paper No. 18-01. Available at SSRN: *https://ssrn.com/abstract=3080322 or http://dx.doi.org/10.2139/ssrn.3080322*
- **Primavera De Filippi and Aaron Wright,** Blockchain and the Law – The Rule of Code (2018) (acknowledging the opportunities of blockchain technologies and arguing that the law needs to catch up, because blockchain could undermine the capacity of governmental authorities to supervise commercial activities and vital government-provided services);
- **Panisi, Federico, Buckley, Ross P. and Arner, Douglas W.,** Blockchain and Public Companies: A Revolution in Share Ownership Transparency, Proxy-Voting and Corporate Governance?, 2 Stanford Journal of Blockchain Law & Policy 2019. Available at SSRN: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3389045*
- **Rodrigues, Usha,** Law and the Blockchain, 104 Iowa L. Rev. 679, 708-27 (2019) (analyzing default rules from corporate, partnership and contract law that could fill the gaps in smart contracts);
- **Schrepel, Thibault,** Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox (June 11, 2018). Georgetown Law Technology Review / 3 Geo. L. Tech. Rev. 281 (2019). Available at SSRN: *https://ssrn.com/abstract=3193576 or http://dx.doi.org/10.2139/ssrn.3193576*
- **Zetzsche, Dirk A., Ross P. Buckley and Douglas W. Arner,** The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain, 2018 U. Ill. L. Rev. 1361, 1382-1402 (arguing that distributed ledger and blockchain is far from an unregulated space since existing doctrines of contract, corporate and partnership law do apply and could establish a blockchain participant's liability).

Smart Contracts

- **Fairfield, Joshua,** Smart Contracts, Bitcoin Bots, and Consumer Protection, 71 Wash. & Lee L. Rev. Online 35, 36 (2014);
- **Hileman, Garrick and Rauchs, Michel,** 2017 Global Blockchain Benchmarking Study (September 22, 2017). Available at SSRN: *https://ssrn.com/abstract=3040224 or http://dx.doi.org/10.2139/ssrn.3040224*
- **Kiviat, Trevor I.,** Note, Beyond Bitcoin: Issues in Regulating Blockchain Transactions, 65 Duke L.J. 569, 605–07 (2015) (discussing a smart contract to trade futures);
- **Kõlvart, Merit, Margus Poola & Addi Rull,** Smart Contracts, in The Future of Law and eTechnologies 133 (Tanel Kerikmäe & Addi Rull eds., 2016);
- **Koulu, Riikka,** Blockchains and Online Dispute Resolutions: Smart Contracts as an Alternative to Enforcement, 13 Scripted 40, 43-69 (2016);
- **Levy, Karen E.C.,** Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law, 3 Engaging Sci., Tech. & Soc'y 1 (2017);
- **Sklaroff, Jeremy M.**, Smart Contracts and the Cost of Inflexibility, 166 U. Pa. L. Rev. 263 (2017) (arguing that human-based contracting is flexible due to inherent incompleteness while machine-based contracting creates new inefficiencies from automation, decentralization and anonymity);
- Werbach, Kevin and Cornell, Nicolas, Contracts Ex Machina, 67 Duke L.J. 313, 367-81 (2017) (arguing that smart contracts, while offering novel possibilities and potential for changing the commercial world, will not displace contract law due to technical limitations and doctrinal concerns).

Fintech Provider Types

Regulatory Bodies and NGOs

- **Andressen, Sevin,** 'Regulatory and Supervisory Issues from Fintech' Speech at Cambridge Centre for Alternative Finance conference on Navigating the Contours of Alternative Finance (29 June 2017) *https://www.fsb.org/wp-content/uploads/Cambridge-Centre-for-Alternative-Finance-Regulatory-and-Supervisory-Issues-from-Fintech.pdf*
- **Armstrong, Patrick,** 'Regtech and Suptech – change for markets and authorities' ESMA Report on Trends, Risks and Vulnerabilities No.1 (2019) 42 *https://www.esma.europa.eu/sites/default/files/library/esma50-report_on_trends_risks_and_vulnerabilities_no1_2019.pdf#page=42*
- **BIS,** Big tech in finance: opportunities and risks (2019) BIS Annual Economic Report.

- **BIS,** Sound Practices – Implications of fintech developments for banks and bank supervisors (February 2018) BIS, BCBS.
- **Bowman, Michelle W.,** Community Banking in the Age of Innovation (11 April 2019) "Fed Family" Luncheon at the Federal Reserve Bank of San Francisco, San Francisco.
- **Broeders, Dirk, & Jermy Prenio,** Innovative technology in financial supervision (suptech) – the experience of early users (July 2018) BIS, FSI Insights on policy implementation No 9.
- **Buch, Claudia,** Digitalization, competition, and financial stability (17 August 2019) Opening remarks, Seminar – Statistics on Fintech – Bring Together Demand and Supply to Measure its Impact, Kuala Lumpur.
- **Carstens, Agustin,** Big tech in finance and new challenges for public policy (4 December 2018) BIS, Keynote, FT Banking Summit, London.
- **Carstens, Agustin,** 'Big tech in finance and new challenges for public policy' FT Banking Summit, London (4 December 2018) *https://www.bis.org/speeches/sp190314.htm*
- **Financial Stability Board,** 'Fintech and market structure in financial services: Market developments and potential financial stability implications' (14 February 2019) *https://www.fsb.org/wp-content/uploads/P140219.pdf*
- **Frost, Jon, Leonardo Gamacorta, Yi Huang, Hyun Song Shin and Pablo Zbinden,** Bigtech and the changing structure of financial intermediation (April 2019) BIS Working Papers No 779.
- **FSI Connect,** Fintech developments in the insurance industry – Executive Summary (BIS).
- **Mourmouras, John,** 'Fin-Regtech: regulatory challenges with emphasis on Europe' Senior Deputy Governor of the Bank of Greece, at Cornell University, New York City (28 February 2019) *https://www.bis.org/review/r190318m.htm*
- **Institute of International Finance,** 'Regtech in Financial services: Technology Solutions for compliance Reporting' (March 2016) *https://www.iif.com/Portals/0/Files/private/iif-regtech_in_financial_services_-_solutions_for_compliance_and_reporting.pdf?ver=2019-01-04-142943-690*
- **Shin, Hyun Song,** 'Big Tech in Finance: opportunities and risks' BIS Annual Economic Report (23 June 2019) *https://www.bis.org/publ/arpdf/ar2019e3.pdf*
- **Toronto Centre,** 'Suptech: Leveraging technology for better Supervision' TC Notes (July 2018) *https://res.torontocentre.org/guidedocs/Suptech%20-%20Leveraging%20Technology%20for%20Better%20Supervision%20FINAL.pdf*
- **Yuen, Arthur,** 'Regtech in the smart banking era – a supervisor's perspective' Deputy Chief Executive of the Hong Kong Monetary Authority, at HKIB Annual Banking Conference 2018, Hong Kong, (27 September 2018) *https://www.bis.org/review/r181012g.pdf*

Academic Literature

- **Arner, Douglas W., Barberis, Janos N. and Buckley, Ross P.,** Fintech, Regtech and the Reconceptualization of Financial Regulation. Northwestern Journal of International Law and Business (Oct. 2016). Available at SSRN: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847806*
- **Arner, Douglas W., Buckley, Ross P. and Zetzsche, Dirk A.,** Fintech for Financial Inclusion: A Framework for Digital Financial Transformation (September 4, 2018). UNSW Law Research Paper No. 18-87; University of Hong Kong Faculty of Law Research Paper No. 2019/001; University of Luxembourg Law Working Paper No. 004-2019. Available at SSRN: *https://ssrn.com/abstract=3245287* or *http://dx.doi.org/10.2139/ssrn.3245287*
- **Arner, Douglas W., Barberis, Janos N. and Buckley, Ross P.,** Fintech and Regtech in a Nutshell, and the Future in a Sandbox (July 1, 2017). CFA Institute Research Foundation Vol. 3, Issue 4, pp. 1-20, July 2017, ISBN: 978-1-944960-25-4; University of Hong Kong Faculty of Law Research Paper No. 2017/040. Available at SSRN: *https://ssrn.com/abstract=3088303* or *http://dx.doi.org/10.2139/ssrn.3088303*
- **Buckley, Ross P. and Mas, Ignacio,** The Coming of Age of Digital Payments as a Field of Expertise (August 25, 2015). Journal of Law, Technology & Policy, Issue 1, pp 71-87, 2016. Available at SSRN: *https://ssrn.com/abstract=1552754* or *http://dx.doi.org/10.2139/ssrn.1552754*
- **Hileman, Garrick and Rauchs, Michel,** 2017 Global Blockchain Benchmarking Study (September 22, 2017). Available at SSRN: *https://ssrn.com/abstract=3040224 or http://dx.doi.org/10.2139/ssrn.3040224*
- **Malady, Louise, Buckley, Ross P. and Tsang, Cheng-Yun,** Regulatory Handbook: The Enabling Regulation of Digital Financial Services (December 1, 2015). Regulatory Handbook: The Enabling Regulation of Digital Financial Services, December 2015; UNSW Law Research Paper No. 2016-05. Available at SSRN: *https://ssrn.com/abstract=2715350*
- **Zetzsche, Dirk A., Buckley, Ross P. and Arner, Douglas W.,** Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses. Available at SSRN: *https://ssrn.com/abstract=3414401*
- **Zetzsche, Dirk A., Ross P. Buckley, Douglas W. Arner and Janos N. Barberis,** From Fintech to Techfin: The Regulatory Challenges of Data-Driven Finance, 14 N.Y.U. J.L. & Bus. 393, 435-443 (2018) (arguing in favor of data-specific adjustments to financial regulations). Available at SSRN: *https://ssrn.com/abstract=2959925*

- **Zetzsche, Dirk A. and Preiner,** Christina, Cross-Border Crowdfunding – Towards a Single Crowdfunding Market for Europe, European Business Organization Law Review (2019). Available at SSRN: *https://ssrn.com/abstract=2991610*
- **Zetzsche, Dirk Andreas and Dewi, Tsany Ratna,** The Paradoxical Case Against Interest Rate Caps for Micro-finance – And: How Fintech and Regtech Resolve the Dilemma (April 17, 2018). University of Luxembourg Law Working 2018-003. Available at SSRN: *https://ssrn.com/abstract=3159202* or *http://dx.doi.org/10.2139/ssrn.3159202*

Fintech Markets

Regulatory Bodies and NGOs

- **Awazu, Luiz, and Pereira da Silva,** Fintech in EMEs: blessing or curse? (5 June 2018) BIS, Panel remarks at CV Meeting of Central Bank Governors of CEMLA – Asuncion, Paraguay.
- **Broeders, Dirk and Jermy Prenio,** Innovative technology in financial supervision (suptech) – the experience of early users (July 2018) BIS, FSI Insights on policy implementation No 9.
- **FSB,** Fintech Credit, Market structure, business models and financial stability implications(22 May 2017) FSB and BIS, Report prepared by a Working Group established by the Committee on the Global Financial System (CGFS) and the Financial Stability Board (FSB).

Academic Literature

- **Arner, Douglas W., Buckley, Ross P. and Zetzsche, Dirk Andreas,** Fintech for Financial Inclusion: A Framework for Digital Financial Transformation. Available at SSRN: *https://ssrn.com/abstract=3245287.*
- **Buckley, Ross P., Arner, Douglas W. and Zetzsche, Dirk Andreas,** Sustainability, Fintech and Financial Inclusion, European Banking Institute Working Paper Series 2019/41. Available at SSRN: *https://ssrn.com/abstract=3387359.*
- **Fenwick, Mark and Vermeulen, Erik P.M.,** Banking and Regulatory Responses to Fintech Revisited: Building the Sustainable Financial Service "Ecosystems" of Tomorrow (September 1, 2019). Available at SSRN: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3446273*
- **Hileman, Garrick and Rauchs, Michel,** 2017 Global Blockchain Benchmarking Study (September 22, 2017). Available at SSRN: *https://ssrn.com/abstract=3040224 or http://dx.doi.org/10.2139/ssrn.3040224_*
- **Kilborn, Jason J.,** Crowdfunding and Crowdlending in the US: Regulations, Exemptions, and Outcomes (April 1, 2019). Available at SSRN: *https://ssrn.com/abstract=3362591 or http://dx.doi.org/10.2139/ssrn.3362591*
- **Nemoto, Naoko, Storey, David J. and Huang, Bihong,** Optimal Regulation of P2P Lending for Small and Medium-Sized Enterprises (January 2, 2019). ADBI Working Paper 912. Available at SSRN: *https://ssrn.com/abstract=3313999* or *http://dx.doi.org/10.2139/ssrn.3313999*
- **Tsai, Chang-hsien,** To Regulate or Not to Regulate? A Comparison of Government Responses to Peer-to-Peer Lending among the United States, China, and Taiwan (2018). University of Cincinnati Law Review, Vol. 87, No. 4, 2018, p. 1077 – 1122 . Available at SSRN: *https://ssrn.com/abstract=3426015*
- **Zetzsche, Dirk A., Buckley, Ross P., Arner, Douglas W. and Barberis, Janos N.,** Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation (August 14, 2017). 23 Fordham Journal of Corporate and Financial Law 31-103 (2017). Available at SSRN: *https://ssrn.com/abstract=3018534.*
- **Zetzsche, Dirk A., Arner, Douglas W., Buckley, Ross P.,** Decentralized Finance (DeFi), Working Paper (2020), *www.ssrn.com/abstract=3539194.*

Fintech: Common Policy and Regulatory Issues

Literature on Fintech for Financial Inclusion

Regulatory Bodies and NGOs

- **Claessens, Stijn, Frost, Jon, Turner, Grant and Feng Zhu,** Fintech credit markets around the world: size, drivers and policy issues (September 2018) BIS Quarterly Review.
- **Brainard, Lael,** Fintech and the Search for Full Stack Financial Inclusion (17 October 2018) Remarks at the Fintech, Financial Inclusion – and the Potential to Transform Financial Services, Boston.
- **Awara, Luiz and Pereira da Zilva,** Financial inclusion in the age of fintech: a paradigm shift (25 October 2018) BIS, Welcoming keynote address, Fourth FSI-GPFI conference, Switzerland.
- **Coeure, Benoit,** Fintech for the people (31 January 2019) BIS, Keynote speech,14th BCBS-FSI high-level meting to Africa, Cape Town.

- **Carstens, Agustin,** Central banking and innovation: partners in the quest for financial inclusion (25 April 2019) BIS, Speech, C D Deshmukh Memorial Lecture, Mumbai.
- **Philippon, Thomas,** The Fintech Opportunity (August 2017) BIS Working Paper No 655.

Academic Literature

Arner, Douglas W., Zetzsche, Dirk Andreas, Buckley, Ross P. and Barberis, Janos Nathan, The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities, European Business Organization Law Review (2019). Available at SSRN: *https://ssrn.com/abstract=3224115*

- **Arner, Douglas W., Buckley, Ross P., and Zetzsche, Dirk Andreas,** Fintech for Financial Inclusion: A Framework for Digital Financial Transformation. Available at SSRN: *https://ssrn.com/abstract=3245287*
- **Buckley, Ross P., Arner, Douglas W. and Zetzsche, Dirk Andreas,** Sustainability, Fintech and Financial Inclusion. Available at SSRN: *https://ssrn.com/abstract=3387359* or
- **Gibson, Evan, Lupo-Pasini, Federico and Buckley, Ross P.,** Regulating Digital Financial Services Agents in Developing Countries to Promote Financial Inclusion, (2015) Singapore Journal of Legal Studies, 26-45. Available at SSRN: *https://ssrn.com/abstract=2973806*
- **Goodell, Geoffrey and Aste, Tomaso,** A Decentralised Digital Identity Architecture (February 23, 2019). Available at SSRN: *https://ssrn.com/abstract=3342238* or *http://dx.doi.org/10.2139/ssrn.3342238*
- **Hockett, Robert C.,** Money's Past is Fintech's Future: Wildcat Crypto, the Digital Dollar, and Citizen Central Banking (December 11, 2018). 2 Stanford Journal of Blockchain Law & Policy (2019). Available at SSRN: *https://ssrn.com/abstract=3299555*
- **Malady, Louise, Buckley, Ross P., Didenko, Anton and Tsang, Cheng-Yun,** A Regulatory Diagnostic toolkit for Digital Financial Services in Emerging Markets (December 1, 2018). (2018) 34 Banking and Finance Law Review 1. Available at SSRN: *https://ssrn.com/abstract=3380885*
- **Malady, Louise, Buckley, Ross P. and Tsang, Cheng-Yun,** Regulatory Handbook: The Enabling Regulation of Digital Financial Services (December 1, 2015). Available at SSRN: *https://ssrn.com/abstract=2715350*
- **Zetzsche, Dirk A. and Dewi, Tsany Ratna,** The Paradoxical Case Against Interest Rate Caps for Microfinance – And: How Fintech and Regtech Resolve the Dilemma (April 17, 2018). University of Luxembourg Law Working 2018-003. Available at SSRN: *https://ssrn.com/abstract=3159202*

Literature on Fintech and Financial Stability Concerns

Regulatory Bodies and NGOs

- Big tech in finance: opportunities and risks (2019) BIS Annual Economic Report.
- **Claudia Buch,** Digitalization, competition, and financial stability (17 August 2019) Opening remarks, Seminar – Statistics on Fintech – Bring Together Demand and Supply to Measure its Impact, Kuala Lumpur.
- Fintech Credit, Market structure, business models and financial stability implications (22 May 2017) FSB and BIS, Report prepared by a Working Group established by the Committee on the Global Financial System (CGFS) and the Financial Stability Board (FSB).
- **Luiz Awazu and Pereira da Silva,** Fintech in EMEs: blessing or curse? (5 June 2018) BIS, Panel remarks at CV Meeting of Central Bank Governors of CEMLA – Asuncion, Paraguay.
- **Luiz Awara and Pereira da Zilva,** Financial inclusion in the age of fintech: a paradigm shift (25 October 2018) BIS, Welcoming keynote address, Fourth FSI-GPFI conference, Switzerland.
- **Luiz Awara, Pereira da Zilva and Goetz von Peter,** Financial instability: can Big Data help connect the dots? (29 November 2018) BIS, Remarks, Ninth European Central Bank Statistics Conference, Frankfurt.
- **Thomas Philippon,** The Fintech Opportunity (August 2017) BIS Working Paper No 655.

Academic Literature

- **Buckley, Ross P., Arner, Douglas W., Zetzsche, Dirk A. and Selga, Eriks**, The Dark Side of Digital Financial Transformation: The New Risks of Fintech and the Rise of TechRisk, Singapore Journal of Legal Studies (2020). Available at SSRN: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478640*

Fintech and Market Integrity Concerns

Academic Literature

- **Arner, Douglas W., Zetzsche, Dirk Andreas and Buckley, Ross P. and Barberis, Janos Nathan,** The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities. European Business Organization Law Review 2019. Available at SSRN: *https://ssrn.com/abstract=3224115*

- **Arner, Douglas W., Barberis, Janos Nathan and Buckley, Ross P.,** The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data. (2016) 44 Journal of Financial Transformation 79. Available at SSRN: *https://ssrn.com/abstract=3044280.*
- **Arner, Douglas W., Barberis, Janos N. and Buckley, Ross P.,** Fintech, Regtech and the Reconceptualization of Financial Regulation. Northwestern Journal of International Law & Business (2017). Available at SSRN: *https://ssrn.com/abstract=2847806*

Literature on Fintech and "Protection" Concerns

Regulatory Bodies and NGOs

- **Awazu, Luiz, and Pereira da Silva,** Fintech in EMEs: blessing or curse? (5 June 2018) BIS, Panel remarks at CV Meeting of Central Bank Governors of CEMLA – Asuncion, Paraguay.
- **CBI,** The need for resilience in the face of disruption: Regulatory expectations in the Digital World, Central Bank of Ireland, Financial Summit, Dublin.
- **Panetta, Fabio,** Fintech and banking: today and tomorrow (12 May 2018) Speech by the Deputy Governor of the Bank of Italy, Rome.

Academic Literature

- **Arner, Douglas W., Buckley, Ross P. and Zetzsche, Dirk Andreas,** Fintech for Financial Inclusion: A Framework for Digital Financial Transformation. Available at SSRN: *https://ssrn.com/abstract=3245287.*
- **Finck, Michèle,** Blockchains and Data Protection in the European Union (November 30, 2017). Max Planck Institute for Innovation & Competition Research Paper No. 18-01. Available at SSRN: *https://ssrn.com/abstract=3080322* or *http://dx.doi.org/10.2139/ssrn.3080322*

Regulatory tools for Further Innovation

Regulatory Bodies and NGOs

- **BIS,** Are post-crisis statistical initiatives completed? (January 2019) BIS IFC Bulletin No 49.
- The use of big data analytics and artificial intelligence in central banking (May 2019) BISIFC Bulletin No 50.
- Sound Practices – Implications of fintech developments for banks and bank supervisors (February 2018) BIS, BCBS.
- **Stijn Claessens, Jon Frost, Grant Turner and Feng Zhu,** Fintech credit markets around the world: size, drivers and policy issues (September 2018) BIS Quarterly Review.
- Financial Stability Board, RSB,
- **Hiroshi Nakaso,** Fintech – its impacts on fiannce, economics and central banking (18 November 2016) Remarks at the University of Tokyo, BIS Central Bankers speeches.
- **Dave Ramsden,** The Bank of England – Open to Fintech (22 March 2018) HMT's International Fintech Conference, London, remarks.
- **Fabio Panetta,** Fintech and banking: today and tomorrow (12 May 2018) Speech by the Deputy Governor of the Bank of Italy, Rome.
- **Jacqueline Loh,** E-payments in Asia – regulating innovation and innovative regulation (26 June 2018) Keynote address at the Central Bank Payments Conference, Singapore.
- **Philip Lowe,** A journey towards a near cashless payments system (26 November 2018) Speech, Australian Payment Summit, Sydney.
- **John (Iannis) Mourmouras,** Fin-Regtech: Regulatory challenges with emphasis on Europe (28 February 2019) Cornell University, New York, Keynote speech.
- **Andrea M Maecler and Thomas Moser,** The evolution of payment systems in the digital age: A central bank perspective (28 March 2019) Swiss National Bank, Money Market Event, Zurich, Speech.
- **Tharman Shanmugaratnam,** Banking liberalisation's next chapter – digital banks (28 June 2019) Keynote Address, The Association of Banks Annual Dinner, Singapore.
- **Claudia Buch,** Digitalization, competition, and financial stability (17 August 2019) Opening remarks, Seminar – Statistics on Fintech – Bring Together Demand and Supply to Measure its Impact, Kuala Lumpur.

Academic Literature

- **Arner, Douglas W., Barberis, Janos Nathan and Buckley, Ross P.,** Fintech and Regtech in a Nutshell, and the Future in a Sandbox (July 1, 2017). CFA Institute Research Foundation Vol. 3, Issue 4, pp. 1-20, July 2017, ISBN: 978-1-944960-25-4; University of Hong Kong Faculty of Law Research Paper No. 2017/040. Available at SSRN: *https://ssrn.com/abstract=3088303* or *http://dx.doi.org/10.2139/ssrn.3088303*
- **Arner, Douglas W., Buckley, Ross P. and Zetzsche, Dirk Andreas,** Fintech for Financial Inclusion: A Framework for Digital Financial Transformation (September 4, 2018). UNSW Law Research Paper No. 18-87; University of Hong Kong Faculty of Law Research Paper No. 2019/001; University of Luxembourg Law Working Paper No. 004-2019. Available at SSRN: *https://ssrn.com/abstract=3245287 or http://dx.doi.org/10.2139/ssrn.3245287*

- **Brummer, Christopher J. and Yadav, Yesha,** Fintech and the Innovation Trilemma (October 17, 2017). 107 Georgetown Law Journal 235, 2019 ; Vanderbilt Law Research Paper No. 17-46; Georgetown Law and Economics Research Paper No. 11-23. Available at SSRN: *https://ssrn.com/abstract=3054770* or *http://dx.doi.org/10.2139/ssrn.3054770*
- **Buckley, Ross P., Arner, Douglas W., Veidt, Robin and Zetzsche, Dirk Andreas,** Building Fintech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond (November 1, 2019). University of Luxembourg Law Working Paper No. 2019-010; European Banking Institute Working Paper Series 2019 – no. 53; UNSW Law Research Paper No. 19-72. Available at SSRN: *https://ssrn.com/abstract=3455872* or *http://dx.doi.org/10.2139/ssrn.3455872_*
- **Chiu, Iris H-Y,** A Rational Regulatory Strategy for Governing Financial Innovation (September 5, 2017). European Journal of Risk Regulation, Forthcoming. Available at SSRN: *https://ssrn.com/abstract=3032712*
- **Fenwick, Mark and Vermeulen, Erik P.M.,** Banking and Regulatory Responses to Fintech Revisited: Building the Sustainable Financial Service "Ecosystems" of Tomorrow (September 1, 2019). Lex Research Topics in Corporate Law & Economics Working Paper no. 2019-4. Available at SSRN: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3446273*
- **Micheler, Eva and Jiang, Johannes,** Regulatory Technology - Eight Policy Recommendations (July 22, 2019). LSE Law - Policy Briefing Paper No. 37, July 2019. Available at SSRN: *https://ssrn.com/abstract=3423899* or *http://dx.doi.org/10.2139/ssrn.3423899*
- **Perlman, Leon,** A Model Crypto-Asset Regulatory Framework (May 16, 2019). Available at SSRN: *https://ssrn.com/abstract=3370679* or *http://dx.doi.org/10.2139/ssrn.3370679*
- **Zetzsche, Dirk Andreas and Buckley, Ross P. and Arner, Douglas W. and Barberis, Janos Nathan,** Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation. 23 Fordham Journal of Corporate and Financial Law 31-103 (2017). Available at SSRN: *https://ssrn.com/abstract=3018534*

Furthering Digital Finance by Other Means

Academic Literature

- **Athreye, Suma S.,** Agglomeration and Growth: A Study of the Cambridge Hi-Tech Cluster (June 2001). SIEPR Discussion paper 00-42. Available at SSRN: *https://ssrn.com/abstract=302958*
- **Maignan, Carole Juliette and Ottaviano, Gianmarco I.P. and Pinelli, Dino,** ICT, Clusters and Regional Cohesion: A Summary of Theoretical and Empirical Research (June 2003). FEEM Working Paper No. 58.2003. Available at SSRN: *https://ssrn.com/abstract=438507* or *http://dx.doi.org/10.2139/ssrn.438507*
- **Mohr, Vivian and Garnsey, Elizabeth W.,** Exploring the Constituents of Growth in a Technology Cluster: Evidence from Cambridge, UK (September 1, 2010). Centre for Technology Management (CTM) Working Paper 2010/01. Available at SSRN: *https://ssrn.com/abstract=1923065* or *http://dx.doi.org/10.2139/ssrn.1923065*
- **Schiavone, Francesco,** The Strategic and Technological Determinants of the Structural Forms of Hi-Tech Clusters (January 22, 2009). International Journal of Technoentrepreneurship, Vol. 1, No. 3, pp. 296-312, 2008. Available at SSRN: *https://ssrn.com/abstract=1331481*
- **Zetzsche, Dirk A., Ross P. Buckley, Douglas W. Arner & Janos N. Barberis,** From Fintech to Techfin: The Regulatory Challenges of Data-Driven Finance, 14 N.Y.U. J.L. & Bus. 393, 435-443 (2018) (arguing in favor of data-specific adjustments to financial regulations). Available at SSRN: *https://ssrn.com/abstract=2959925.*
- **Zetzsche, Dirk Andreas and Arner, Douglas W. and Buckley, Ross P. and Weber, Rolf H.,** The Future of Data-Driven Finance and Regtech: Lessons from EU Big Bang II (March 27, 2019). European Banking Institute Working Paper Series 2019/35. Available at SSRN: *https://ssrn.com/abstract=3359399* or *http://dx.doi.org/10.2139/ssrn.3359399*

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