Finance, Competitiveness, and Innovation Global Practice, World Bank
Financial Institutions Group, International Finance Corporation

Regulation and Supervision of Fintech: Considerations for EMDE Policymakers

Fintech and the Future of Finance Flagship Technical Note

WORLD BANK GROUP

Regulation and Supervision of Fintech: Considerations for EMDE Policymakers

Fintech and the Future of Finance Flagship Technical Note

WORLD BANK GROUP

1818 H Street NW,
Washington DC 20433
Telephone: 202-473-1000;
Internet: www.worldbank.org

Contents

List of Figures

List of Boxes

Authors and Contributors

This note is part of a series of technical notes developed for the “Fintech and the Future of Finance” report, a joint effort by the World Bank and the International Finance Corporation (IFC). This project was led by Erik Feyen and Harish Natarajan (both World Bank) and Matthew Saal (IFC) under the overall guidance of Jean Pesme, Mahesh Uttamchandani, and Anderson Caputo Silva (all World Bank) and Paulo de Bolle and Martin Holtmann (both IFC). Alfonso Garcia Mora (IFC, formerly World Bank) provided guidance at inception and during earlier stages of the report.

The note has been authored by Tatiana Alonso Gispert, Pierre-Laurent Chatain, Karl Driessen, Danilo Palermo, and Ariadne Plaitakis. Other contributors are Ana M. Carvajal and Matei Dohotaru.

The team is grateful for extensive peer review comments received from Sharmista Appaya, Mariano Cortes, Denise Dias, Erik Feyen, Katia d’Hulster, Juan Carlos Izaguirre, Yira Mascaró, Cedric Mousset, Harish Natarajan, Jean Pesme, Mathew Saal (all World Bank); and Marc Dobler, Dirk Jan Grolleman, David Hoelscher, Vikram Haksar, Fabiana Melo, Jan Nolte, Parma Bains, and Nobusayu Suhimoto (all IMF).

The team thanks Machimanda A. Deviah (World Bank) for editorial assistance, Maria Lopez (World Bank) and Sensical Design for design and layout, Elizabeth Price, Melissa Knutson and Nandita Roy (all World Bank) and Henry Pulizzi and Elena Gox (both IFC) for communications support, and Michael Geller and Arpita Sarkar (both World Bank) for overall coordination.

Acronyms

API	Application Programming Interface
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
BCBS	Basel Committee on Banking Supervision
BCP	Basel Core Principles for Effective Banking Supervision
BFA	Bali Fintech Agenda
CBDC	Central Bank Digital Currency
DGS	Deposit Guarantee Scheme
DLT	Distributed Ledger Technology
EMDEs	Emerging Market and Developing Economies
EMI	E-Money Institution
FATF	Financial Action Task Force
FSB	Financial Stability Board
FSI	Financial Stability Institute
FX	Foreign Exchange
IMF	International Monetary Fund
KYC	Know-Your-Customer
MoU	Memorandum of Understanding
P2P	Peer to Peer
WB	World Bank

Executive Summary

Fintech is transforming the global financial landscape. It is creating new opportunities to advance financial inclusion and development in Emerging Markets and Developing Economies (EMDEs), but also presents risks that require updated supervision policy frameworks. Fintech encompasses new financial digital products and services enabled by new technologies and policies.[1] Although technology has long played a key role in finance, recent fintech developments are generating disruptive innovation in data collection, processing, and analytics. They are helping to introduce new relationship models and distribution channels that challenge traditional ways of finance, while creating additional risks. While most of these risks are not new, their effects and the way they materialize and spread across the system are not yet fully understood, posing new challenges to regulators and supervisors. For example, operational risk, especially cyber risk, is amplified as increasing numbers of customers access the financial network on a 24/7 basis. Likewise, increased reliance by financial firms on third parties for provision of digital services, such as cloud computing, may lead to new forms of systemic risks and concentration on new dominant unregulated players such as big tech firms.[2]

This note aims to provide EMDE regulators and supervisors with high-level guidance on how to approach the regulating and supervising of fintech, and more specific advice on a few topics. Preserving the stability, safety, and integrity of the financial system requires increased attention to competition and ensuring a level playing field and to emerging data privacy risks. As a general principle, policy response should be proportionate to risks posed by the fintech activity and its provider. While striking the right balance can be challenging in the absence of global standards, the IMF-World Bank Bali Fintech Agenda (BFA), along with guidance by Standard Setting Bodies, provides a good framework for reference.

A sound policy design must start with assessment of the fintech landscape, its risks and regulatory gaps. Simplicity and pragmatism—for example combining simple regulations with supervisory judgment—increases the odds of successful policy. In practice, this will mean different things, depending on local context. In many cases, a clarification or review of existing frameworks will be sufficient and is easily done through enhanced supervisory guidance. In others, a full regulatory overhaul might be required. In some systems, an activities-based, technology-neutral approach, based on the function of the financial service can help balance stability and innovation goals. In others, a combined approach, taking into account the activity and the entity, might be necessary to ensure financial stability. In any case, there needs to be clear definition of which activities are under the regulatory perimeter and which requirements apply, including the need for licenses. Some fintech activities will require licences with integrity (AML/CFT) and conduct requirements. The introduction of data protection provisions in licensing frameworks is common. Activities that could potentially pose risks to stability should face prudential requirements.

Competition and inclusion objectives will become more relevant from a financial policy view, given the growing interdependencies and trade-offs with core priority mandates of preserving stability, integrity, and safety of the financial sector. The multiplicity of new entrants and the potential for dominant players (for example, incumbents, big tech firms, platforms) and first movers (for example, M-Pesa) to create barriers and generate distortions has led to an increased

1. According to the Bali Fintech Agenda and the Financial Stability Board.
2. According to the FSB, big tech firms are large companies with established technology platforms, such as Alibaba, Amazon, Apple, Baidu, eBay, Facebook, Google, and Microsoft. Big techs that offer financial services are a subset of fintech firms—a broader class of technology firms (many of which are smaller than big tech firms) that offer financial services.

recognition of the strong links between inclusion, competition, and financial stability. Indeed, a targeted participation by financial service authorities in competition policy matters is increasingly being observed in EMDEs. The potential role of prudential and conduct regulation in mitigating barriers to market access and reining in abusive dominant practices should not be understated.

Cooperation, both interagency and cross-border, can help in the design and implementation of a sound supervisory response to fintech, which can be particularly challenging for EMDE countries suffering from supervisory capacity constraints or juggling competing policy priorities. An effective supervisory function for fintech activities is as essential as an appropriate regulatory regime. Supervisory processes and methods may need significant changes. Supervisors' knowledge, skills, and tools should keep pace with the speed of innovation and related risks, including cyber threats. Building proper expertise is crucial and suptech and regtech solutions could be excellent catalysts for this. Fintech is cross-sectoral and cross-country, making cooperation among agencies at the national and international levels essential for sound supervision. While many supervisors in G20 EMDEs participate in international fora, smaller jurisdictions may need to rely on International Financial Institutions (IFIs) and other available channels—for example, Global Financial Innovation Network (GFIN)—to raise issues, keep abreast of global developments, and exchange best practices. Involving the industry in fintech policy coordination efforts in a responsible and transparent way also appears increasingly relevant in areas such as cybersecurity, data, payments and securities, and for the design and implementation of regtech and suptech solutions (Appaya et al., 2020).

Further, authorities need to ensure that client funds are well preserved and that proper wind-down mechanisms are in place for systemically relevant firms operating in fintech. For crisis-management, fintech providers should be treated the same as their peers in traditional finance. For E-Money Institutions (EMIs) and payment institutions, regardless of their size, mechanisms should be established to require adequate ring-fencing of client funds and proper segregation, preferably by keeping them in government securities or deposited with the central banks. Where this is not feasible, segregation could be done by requiring that the funds are deposited with commercial banks, although this bears the risk of the commercial banks' failure, in which case the reserves could be lost. To mitigate this risk, some countries extend deposit-insurer protection to EMI customers, although challenges remain for the implementation of such protection, including that it would not cover the risk of misappropriation or fraud by the EMI as the EMI would not be a direct member of the deposit insurer. Other jurisdictions require that the EMI becomes a direct member of the deposit insurer—thus covering losses due to fraud or misappropriation. But this might clash with the purpose of a deposit insurance and impose costs that are not compatible with EMI business models or pose operational challenges that may render them ineffective.

Reaping the benefits from fintech in a sustainable and durable way will require adapting and strengthening financial-policy frameworks. Policymakers need to put in place a timely and proportionate regulatory and supervisory approach to managing financial risks arising from fintech. Ensuring financial stability, safety, and integrity will remain the core mandates, and these can, in turn, contribute to sustainable development amid healthy innovation and increased competition. Assessing the fintech landscape and related risks is a prerequisite to identifying regulatory gaps at an early stage. Then, authorities can set clear policy goals with a priority on surveillance and oversight mandates. As operational risks are amplified, defining a clear strategy for promoting operational resilience is important. Fintech-related changes may also require financial supervisors to scale up capacity and resources to meet the specific challenges posed by fintech, including through use of regtech and suptech solutions. Domestic and international cooperation is essential to successfully manage cross-sectoral risks, while achieving the benefits of fintech. And if an e-money institution fails, authorities should be well prepared by establishing safe mechanisms to protect customers' funds and to wind down systemic fintech firms.

1. Introduction

Fintech is rapidly transforming the global financial landscape, pushing the agenda for development and inclusion in EMDES. Fintech's potential benefits include: (i) increased interoperability and digital identification; (ii) increased efficiency, with lower costs and better data to understand consumer behavior and needs; and (iii) increased competition, with a wider variety of players and services being offered at a generally lower cost. As such, these benefits could help transcend some of the archetypal barriers to financial development and growth in EMDEs, including low formality and inclusion levels, highly concentrated bank-centric sectors, isolated and financially illiterate populations, and institutional capacity constraints (IMF-World Bank Bali Fintech Agenda, 2018, Pereira da Silva, 2018, Philippon, 2016, 2019, World Bank, 2020a).

As fintech adoption increases, so does the need for sound policy frameworks and supervision. Since 2017, the Financial Stability Board (FSB) has monitored the evolution of fintech from a financial stability perspective and has recognized fintech's potential to catalyze permanent and significant changes in finance (FSB, 2019a) and generate important risks once the scale of its adoption reaches a certain threshold (globally or in important nodes of the global financial markets). The World Bank's *Digital Financial Services* white paper (April 2020), lays out four broad stages of digital transformation of financial services, ranging from access to basic transaction accounts to a fully digital financial system. These stages tend to be accompanied by increasingly developed legal and regulatory frameworks, enabling infrastructures, and ancillary government support systems. As such, the richness and complexity of the policy response will, and must, increase as more fintech activities become available and more broadly used.

Despite the lack of global standards for (or adapted to) fintech, countries seeking to embrace the fintech promise must adopt appropriate regulatory and supervisory arrangements. According to Pazarbasioglu et al. (2020) the policy response to fintech should aim at: (i) identifying, mitigating and addressing risks to financial stability and integrity, (ii) safeguarding consumer protection (iii) enabling new players and approaches, (iv) promoting competition, and (vi) fostering consumer demand and confidence. But designing and implementing such a balanced policy response can be challenging in the absence of global standards. Fortuitously, the World Bank-IMF Bali Fintech agenda (BFA) and emerging high-level guidance by the Standard Setters have provided a safe bridge until these emerge. The main pillars of the BFA are: (i) adopting basic regulatory principles for fintech, (ii) ensuring regulatory certainty and clarity and reviewing/supplementing existing regulatory approaches to address new challenges posed by fintech, (iii) formulating a holistic policy response guided by certain basic regulatory principles, such as technological neutrality and risk proportionality; and (iv) upgrading the legal framework to provide an enabling legal landscape. Additionally, guidance from global standard setting bodies—such as the Basel Committee on Banking Supervision (BCBS) on how to apply the Basel Core Principles (BCPs) for Effective Banking Supervision to e-money in BCBS 2016; high-level Financial Stability Board (FSB) global stablecoin recommendations in FSB 2020a; and the Financial Action Task Force (FATF) recommendation for virtual assets service providers in FATF 2019—provide critical foundational steps to support development of sound regulatory and supervisory frameworks for fintech. However, chronic issues that many EMDEs suffer from,[3] such as poor institutional frameworks and capacity constraints, can jeopardize a country's ability to tackle existing and prospective financial risks properly.

3. These include the following: (i) Low levels of financial and technological development; (ii) Low levels of financial inclusion and literacy; (iii) Bank-centric and highly concentrated banking sectors with low efficiency and competition levels; (iv) Weak or compromised institutional frameworks prone to regulatory uncertainty and capture; and (v) Potentially conflicting mandates for financial authorities.

The main objective of this note is to offer EMDE policymakers strategic considerations on how to provide an adequate policy response to fintech, including in case of failure of fintech providers. The note reviews the main vectors of risk arising from fintech adoption and the main elements that an adequate policy response should include to ensure that these risks are adequately monitored and contained. Several EMDEs have been supportive of fintech and stand out as frontrunners in activities such as e-money or digital payments. A selection of these experiences is documented in this note (including in the appendix), illustrating the range of policy options adopted thus far and the potential for expanding opportunities for South-South cooperation and information exchange. Unless stated otherwise (for example, specific deep dives and case studies), the strategic considerations and advice offered in this note apply to the whole fintech ecosystem, including all fintech activities,[4] and incumbent and new fintech firms.

The note has the following structure. Section 2 discusses the main risks posed by fintech, with particular attention to operational risks, especially those arising from the outsourcing of technological services to third parties. This section also documents several examples of recent fintech failures. Section 3 describes the main regulatory strategies and approaches that authorities can follow when deciding when and how to regulate fintech. Deep dives in this section include innovation facilitators in Asia, the regulation of crowdfunding around the world and of digital money in Africa, reflections related to competition aspects and a discussion on designing proportional licensing frameworks. Section 4 discusses the main challenges that EMDE supervisors may encounter as fintech adoption accelerates in their countries, with focused discussions on capacity constraints and on the need to collaborate, both at the local and global level, to overcome some of these challenges. Section 5 discusses whether and how to protect customers' funds and financial stability when a fintech firm fails and how to establish appropriate wind-down mechanisms for e-money providers. Section 6 concludes with a set of high-level recommendations.

4. According to the Bali Fintech Agenda and the Financial Stability Board—which subsequently added a materiality condition—fintech is the *group of all advances in technology, as well as associated new business models, applications, processes, and products in finance that have a material effect on the provision of financial services.* In this note, we refer to "fintech activities" as the set of financial services that are provided using fintech technologies.

2. Fintech Risks

Fintech risks are similar in nature to those of traditional financial activities, but their pace of materialization and impact can differ significantly. Policy makers, researchers, and international bodies agree that, because the intermediary and transformation functions provided are still the same (payment, saving, investment, credit, advice, etc.), the main risks arising from fintech activities are not dissimilar to those arising from more traditional financial business models. For firms (incumbents or new entrants) these comprise legal, reputational, governance, integrity, and operational risks. Depending on the business model (especially if the firms hold client funds) credit, market, and liquidity risks will arise. Risks to consumers include mis-selling of products and services, financial exclusion, data privacy, security risks, or abusive behavior.[5] The intensity and manner in which these risks materialize and spread across the system can vary depending on a long list of factors, including the business model, the distribution channel, the legal status and regulation of the providers, and the nature and degree of adoption of the activity performed.

New entrants operating exclusively in the digital space appear more vulnerable to certain risks such as misconduct and fraud, integrity risks, cyberattacks, or lack of solvency due to undercapitalization. The world of fintech is made of sterling success stories, but it also has its dark side. In an increasingly competitive environment, many fintech startups fail every year for different reasons, including lack of financial strength, low demand, or a flawed business case. These failures have left behind unpaid staff, customers out of pocket, and investors facing deep losses.[6] In a few instances, the impact has been huge, triggering reputational issues as doubts were cast on the quality of regulation and oversight. There have also been failures related to fraud and market misconduct and abusive practices (box 1). Understanding and monitoring these risks can be challenging for a supervisor hampered by capacity constraints or being unaware of the transformative changes that new technologies may imprint on financial market dynamics.

Risks to consumer protection and financial integrity can be substantially exacerbated in a financial landscape with significant fintech presence. Due to the digital form of fintech products and services, there is often limited electronic disclosure of terms and conditions and lack of transparency of costs and business model. For example, online payday loans look harmless at first sight due to the small amount of money involved and the flexibility for the client to repay. They are also usually approved with almost no customer due diligence. Further, the loans are sometimes granted to hard-pressed borrowers unable to gain credit elsewhere. Still, thousands of customers have ended up being trapped in debt due to rapid interest accumulation, hidden penalty charges, and rollover fees. Many customers and investors are lured by highly attractive investment products that turn out to be fraudulent (box 1). In some cases, supervisors overlooked the red flags for too long or lacked the authority to protect customers because service providers were outside their purview.

Fintech activities carry important integrity risks such as identity theft and online extortion (for example, ransomware attacks). Money laundering and financing of terrorism practices can proliferate amid digital financial platforms that facilitate anonymity in transactions. The use of crypto-assets, increasingly popular in EMDEs, raises big concerns, for example. Several high-profile cases of criminal activities[7] have surfaced in recent years attracting the authorities' attention and prompting intervention of the AML/CFT global standard setter, FATF, with issuance of new specific recommendations for virtual assets service providers (FATF 2019).

5. The risks associated with fintech have already been identified and described in several reference papers. See for example FSB 2017a, FSB 2019, BCBS 2018.
6. The fintech firms that went out of business in 2019, by Oliver Smith, AltFi, December 27, 2019.
7. See, for example, the case of Crypto Capital Corporation of Poland that held bank accounts in a small rural bank and laundered illegal proceeds through a cryptocurrency exchange firm; for further details: Electronic Money Laundering, The Dark Side of Fintech. An Overview of the Most Recent Cases, ICIME 2020: 2020 12th International Conference on Information Management and Engineering.

In a context where data is highly valued and instrumental for most fintech businesses, the risks of inappropriate commercial uses or disclosure of consumer data is high. Fintech activities often involve collection, storage, processing, analysis, and exchange of consumer data by a variety of players, incumbent firms, and fintech startups. These exchanges expose consumers to the risk of unauthorized disclosure and use of their personal data, including fraud and identify theft. In addition, data limitations may make it difficult for firms to validate outcomes, not least where artificial intelligence (AI) is used to analyze data sets and generate solutions.[8] Data breaches can result in customers losing trust in fintech firms and financial services more broadly. While Customer Due Diligence (CDD)/Know Your Client (KYC) procedures are well developed in the banking industry, they can be much less, if at all, in alternative channels. As distribution is by a digital device, there is often no face-to-face interaction with providers that might help ensure appropriateness of a product or service. This may increase the likelihood of abusive behaviour, fraud, and operational failures, which reduces trust in fintech and undermines its adoption (Pazarbasioglu et al., 2020).

Box 1. Examples of Failures of Fintech Firms Involving Fraud, Misconduct, or Abusive Practices

Wirecard AG (Germany, 2020): A well-known fintech failure is that of the German DAX listed tech champion Wirecard AG, which filed for bankruptcy in June 2020 in the wake of a big accounting scandal. The company was an international supplier of electronic-payment and risk-management services and also provided financial services to both business and private customers through Wirecard Bank AG, a fully licensed German bank supervised by Bafin, the German Federal Financial Supervisory Authority.[9] In the area of mobile payments, Wirecard AG developed a fully digitalized mobile-payment app called Boon, which allowed customers to make contactless payments on the go, using their mobile phones or smartwatches. It was also active in e-commerce, digitization of the retail sector, and finance technology through partnerships with fintech companies like Curve, Funding Circle, startup banks (Atom), and money apps, including Revolut and Pockit. The company had developed its business worldwide with operations in Australia, China, Singapore, Turkey, the United Kingdom, and the U.S. In June 2020, it reported €1.9 billion cash missing from the company's accounts following an audit by Ernst & Young. Its CEO resigned and was arrested by the German police for "inflating Wirecard AG's sales volume with fake income."[10] According to external sources, half of its global revenue and almost all the reported profits came from three opaque partner companies.[11]

The collapse of Wirecard affected a myriad of fintech partners offering banking and payment services (Pockit, Curve, CardOneMoney, Payoneer, Revolut, Soldo, and BBVA-owned Holvi). Millions of customers were unable to access their funds (including paid-in salaries) as their accounts and bank cards were suspended.[12] The company's auditors have faced legal action for failure to flag improperly booked payments on Wirecard's 2018 accounts. The question of why the supervisory authorities were not able to detect this fraud on time remains unanswered but the fintech factor is likely to have played a relevant role given the complexity of a business model that was unfamiliar to supervisors and auditors alike.[13]

Wonga (UK, 2018). Wonga was a payday-lending company based in the United Kingdom. In 2010, it launched a product for online borrowers seeking short-term credit. The automated, user-friendly, platform offered a 24/7 service, instant approval, and immediate fulfillment.[14] In exchange, customers paid very high interest rates. The company grew quickly, backed by private equity investors, and was renowned as one of a new breed of digital

8. KPMG (2019), "Regulation and supervision of fintech".
9. Wirecard Bank AG is not part of the insolvency proceedings of Wirecard AG. On June 26, 2020 the United Kingdom's FCA ordered the suspension of Wirecard Card Solutions Limited (WCS), a subsidiary of Wirecard, which handled payment processing and issued cards for a number of banking services in the U.K. and across Europe.
10. Wirecard's Former CEO Markus Braun Is Arrested. The Wall Street Journal, June 23, 2020.
11. https://www.ft.com/content/a7b43142-6675-11e9-9adc-98bf1d35a056
12. Wirecard Collapse Freezes Millions of Online Bank Accounts: Will Customers Ever Get Their Money Back? Barry Collins, Forbes, June 28, 2020.
13. Wirecard Scandals leaves German Regulators under Fire. Olaf Storbeck and Guy Chazan, FT, June 26, 2020.
14. Fintech Payday Lending: The Case of Wonga. Yashi Wang, September 18, 2019.

innovators in the finance industry. At the height of its success around 2012, Wonga was delivering £1.2 billion of loans and posted a net profit of £62.5 million. The company started to come under the authorities' scrutiny due to its aggressive debt collection tactics and questionable advertisement spots. Further, pressure started to build against payday lenders as stories emerged of vulnerable customers struggling to repay. In 2013, Wonga raised its Annual Percentage Rate (APR) to 5853 percent, which prompted authorities to react and put a cap on the total cost of a loan. The company suffered an exceptional surge in customer compensation claims and collapsed in 2018. According to the latest developments, many borrowers have complained about too a little compensation and not being eligible for the Financial Services Compensation Scheme.[15]

Ezubao (China, 2016). Between 2014 and 2017, China's growth in peer-to-peer (P2P) lending platforms skyrocketed, with volumes surpassing those in the US. In a widely fragmented market (with more than 4000 lending platforms at the peak) several local finance companies thrived offering loans to underserved individuals. But in the second half of 2018 the P2P market shrank dramatically[16] amid tightening regulations and oversight to contain the speculative frenzy and stop an epidemic of fraud and weakening investor sentiment fueled by massive defaults.[17] The case of Ezubao, one of China's largest P2P lending platforms, is emblematic; 95 percent of its investment products were fake. The nearly one million investors that fell for promises of annual interest payments of 15 percent lost $7.6 billion collectively in what was the second largest Ponzi scheme in history (after Madoff's). As more cases of illegal fund-raising in P2P lending platforms occurred, the Chinese authorities adopted aggressive measures to tighten the regulation of the industry, introducing strict P2P licensing requirements in 2019.

Trustbuddy (Sweden, 2015). This was the world's first listed P2P lending platform to file for bankruptcy and be delisted from the stock exchange in October 2015 after a newly arrived management team uncovered evidence of serious misconduct. The Swedish platform had been using lenders' capital "in violation of their instructions" or without their permission and the clients' money had not been held separately from the TrustBuddy company account. The investigation revealed a £3.5 million discrepancy between the amount owed to investors and the available balance of client bank accounts. Moreover, existing loans, some non-performing, had been reassigned to new capital deployed by lenders, thereby disguising poor performance.[18] During the liquidation process, there was a much discussion around whether the outstanding loan book was a (segregated) property of the lenders or not, and whether the assets should be pursued or sold off.

Cyber risks can be exacerbated in a financial sector with significant fintech activity as new digital distribution channels expand the network and make it vulnerable to attacks. Recent cyberattacks show that security breaches may compromise business continuity, carry enormous economic and reputational risks, and threaten financial stability (FSB 2020b). In EMDEs, where the payment and financial market infrastructure is often less resilient than in advanced economies, the probability and impact of cyberattacks is higher. Moreover, as the user base of digital platforms increases, especially for payments, so does the exploiting of vulnerabilities, including in encryption and interfaces.

Another source of increasing operational risk is the higher reliance on third-party service providers such as cloud-computing firms. Banks and other traditional financial institutions have outsourced services to third parties for decades but, in recent years, the extent and nature of these interactions has intensified, particularly in technology services and cloud computing. Regulated firms are subject to prudential regulations that force them to manage outsourcing risks[19]

15. Wonga Compensation, an Insult to Borrowers. BBC, https://www.bbc.com/news/business-51303908.
16. The Meteoric Rise and Spectacular Fall of Peer-to-Peer Lending in China, the World's Largest Peer-to-Peer Lending Market may Soon Cease to Exist. Peter Renton, Lendacademy, October 23, 2019.
17. China's P2P Lending Market could be Decimated this Year amid Beijing Crackdown. Orange Wang and Chad Bray, South China Morning Post, April 15, 2019.
18. Tales of Failed Peer-to-Peer Lenders. Ryan Weeks, AltFi, March 2, 2018.
19. The entity delegates control over risk management to the third party but remains responsible for it.

but unregulated firms are not. According to the FSB (FSB 2020d), increased operational risks due to higher reliance on third-party providers could become systemic, calling for a regulatory and supervisory response to ensure that adequate risk-control mechanisms are in place, including due diligence procedures, operational risk management, ongoing monitoring, and an appropriate execution of contracts assigning responsibilities, agreed service levels, and audit rights.

Multiple unregulated fintech firms have gone out of business because of insufficient funds and/or lack of experience in the financial sector, especially with respect to regulatory and compliance issues. Many fintech companies require strong IT infrastructures and expertise in technology, risk management, and finance. But all these elements come at a cost that new entrants may not necessarily afford. One example is the need for extensive legal counsel to understand and remain compliant with the many rules and regulations governing the financial industry. Having adequate capital up front is essential together with a realistic business plan, but unregulated fintech firms may lack the capacity to raise sufficient funds to cover a critical mass of clients. Plastc was a fintech startup launched in 2014 with the ambition to develop a smart card able to store information from several credit/debit cards in one. In 2014 the company raised more than $9 million, but three years later it went bankrupt, unable to raise enough money to move the product to mass-production[20]. Likewise, the culture of compliance and risk management in a fintech firm might not be as strong and rooted as it is in banks and regulated financial institutions.[21] In fact, many fintech startups have entered the market without having the right background and expertise in finance, which hinders their ability to develop sound credit-undertaking practices[22] or realize the potential scale of compliance costs once regulated. For example, BitLendingClub, a peer-to-peer Bitcoin lending platform terminated its services in 2016 invoking regulatory pressure. BTCjam, a U.S.-based peer-to-peer lending service aiming to provide “unbankable” clients with access to fair and affordable credit in bitcoins shut down in 2017 citing capacity constraints.

20. “Fintech ‘Plastc’ Shuts Down After Cancelling All 80,000 Pre Orders”, Regina Mihindukulasuriya, BW Disrupt, May 2017
21. A prominent U.K.-based fintech valued at $5.5 billion was questioned by its regulators over weak risks’ internal controls and the company responded by hiring former bankers to join its management and compliance teams. A U.S.-based fintech company providing online lending is being investigated for failing to perform AML/CFT due diligence after a terrorist attack was conducted on the U.S. soil.
22. The case of “SameDayCash” is a good example in that regard; in only a few months of existence, the site, which delivered the internet’s first fully automated loans to clients across the U.K., faced default rates of roughly 50 percent due to insufficient credit underwriting standards.

3. Defining the Regulatory Approach

A proportionate and targeted regulatory framework will help keep fintech risks within tolerable levels while promoting innovation, competition, and development. Given the risks posed by fintech, a response from the regulators and supervisors is warranted to ensure that the surveillance and oversight framework for the financial sector continues to fulfill its three core mandates, namely stability, integrity, and safety. Typically, the response will depend on the maturity, degree of adoption and risks of the fintech ecosystem, the country's legal framework, the existing regulatory and supervisory setting, and the prospective institutional capacity. Based on observed practice, responses thus far have ranged from making no changes or marginal ones to existing frameworks to instituting radical overhauls, with some interesting experiences emerging from low and middle-income countries. The three main questions that authorities will face are: (i) What activities and firms to regulate?; (ii) When to impose full regulation and how to accompany the firms earlier through monitoring and testing when risks are not high?; and (iii) How to regulate the identified activities and firms once it is needed?

3.1 What to Regulate?

The nature and risks of the fintech activity will determine whether and how intensely the activity and its provider should be under the purview of the supervisor. As a general principle, any fintech firm that carries out a regulated activity should fall in the regulatory perimeter and be regulated and supervised as a provider of that service. In addition, under a risk-based approach, a non-exhaustive list of considerations would include: (i) the nature of the activity being conducted, (ii) the size of the market, and (iii) potential risks if left outside the perimeter, including for consumers, financial markets, and overall financial stability due to its interlinkages (in some cases, a fintech activity may entail few risks in isolation but when provided by a firm that carries many other activities, the risks can become systemic).

Leaving fintech firms or activities out of the regulatory perimeter can entail significant risks. A lack of surveillance and oversight can hinder the regulators' ability to identify relevant risks posed by a fintech activity early to avoid accumulation of risks outside the regulated perimeter. This situation can end up jeopardizing financial stability and eventually lower economic efficiency and growth (Frost, 2020) as the level playing field is eroded due to regulatory arbitrage by unregulated firms. On another note, regulatory uncertainty may discourage prospective investors and new providers from entering the market if the case for regulation seems clear, but the authorities fail to deploy a credible strategy.

A mechanism to monitor the evolution of risks is needed for fintech activities outside the supervisor's purview. Ideally the jurisdiction would undertake legislative change to extend the financial authority's mandate over that particular activity,[23] but this is not always legally or politically feasible. One alternative is to require a partnership between the entity outside of the perimeter and an entity within the perimeter to allow fintech activity.[24] If the entity outside the regulator's mandate creates a subsidiary dedicated to the activity that is licensed, the regulator can extend its jurisdiction over those subsidiaries through the licensing framework.[25] Another option is a Memorandum of Understanding (MoU) between the

23. For example, the Central Bank of Brazil was recently given a mandate over payment institutions by Law.
24. In Bangladesh non-banks must partner with financial institutions and create a subsidiary to issue e-money.
25. India's Payment Banks can include subsidiaries of Mobile Network Operators (MNOs).

regulator and the entity, with the entity willingly subjecting itself to regulation. This is an approach taken in jurisdictions where entities that are outside the regulatory jurisdiction of central banks/banking supervisors, such as the post office, can offer financial services under a separate statutory act. For example, Bangladesh Bank recently brought a mobile money service launched by Bangladesh Post under its purview through such an MoU approach. Another option involves imposing outsourcing/third-party requirements on the regulated entity that is purchasing services from a tech firm (for example, to monitor suspicious transactions).

3.2 When to Regulate?

There are different, non-mutually exclusive, ways to approach regulation of a fintech activity. These are (i) Regulate; (ii) Wait and See; and (iii) Test and Learn (World Bank, 2020a). In the first case, the regulator is fully persuaded that the fintech activity must be under its purview. If the existing framework does not allow for such coverage, the regulator will either revise it (recommended, see below) or set up a new bespoke one (in some cases the best option, but not always). Options (ii) and (iii) have been adopted when there is regulatory ambiguity concerning the fintech activity, when there is a need to survey the market and, most importantly, to build supervisory capacity in regard to the technology prior to a regulatory response. A Wait and See approach is indicated when there is no evidence that the activity should be regulated and should be ideally complemented by some supervisory monitoring, as explained below. When the situation is such that prospective risks are potentially relevant, but the degree of market penetration is still low, the authorities might decide to opt for the Test and Learn option and implement some form of innovation facilitator (regulatory sandbox, incubator, innovation office and/or hub) to help progressively fill in the regulatory gap.

Some authorities have allowed individual business cases to operate in a live environment with no regulation and some monitoring. In China, mobile payments remained largely unregulated for several years but were monitored until authorities took regulatory action in 2018 in view of the increasing risks posed (box 1). Some authorities have opted to issue a permissive instrument that will often limit the firm's activities to minimize risks and require some information for monitoring purposes (for example, the Central Bank of Kenya issued "letters of no objection" to mobile-money issuers in 2007). One drawback of these approaches is that getting data from unregulated firms can be challenging. Lack of quality data may undermine the supervisor's ability to understand the activity and identify and monitor risks. Authorities need to carefully consider this tradeoff between potential risks and benefits in allowing the activity with no clear regulation and reporting obligations. When, based on the best data available, penetration rates or risks exceed a threshold, a proactive regulatory stance would be warranted.

A common first step towards setting a regulatory and supervisory framework for fintech is the establishment of innovation facilitators such as innovation offices or regulatory sandboxes. Innovation offices or hubs provide a regulatory touchpoint for firms and allow supervisors to monitor developments and provide guidance where necessary. Sandboxes and innovation accelerators allow individual business cases to operate in a live environment under close monitoring (see box 2 and appendix). Although resource-intensive, they can provide support, advice, guidance, and physical space for fintech firms to identify opportunities for growth and navigate the regulatory, supervisory, and legal environment (World Bank 2020). They also help inform policy and strategic decisions in different ways. For example, accelerators are largely used to foster a fintech ecosystem within a jurisdiction while sandboxes help understand the risks involved in a fintech activity and test the appropriate regulation at a reduced scale. For example, Hong Kong SAR, China's Fintech Supervisory Sandbox allows banks and their partnering tech firms to conduct pilot trials of their fintech initiatives involving a limited number of participating customers without the need for full compliance with the HKMA's supervisory requirements.[26]

26 See the HKMA's website here for more details.

Box 2. Innovation Facilitators in Asia

Malaysia's central bank's first step in supporting financial innovation was establishing a Financial Technology Enabler Group in June 2016. This Group launched a fintech regulatory sandbox in October 2016 that permits the testing of innovative products, services, and business models that are designed to (i) improve accessibility, efficiency, security, and quality in the provision of financial services; (ii) enhance the efficiency and effectiveness of Malaysian financial institutions' management of risks; and (iii) address gaps in or open up new opportunities for financing or investments in the Malaysian economy. In May 2017, digital remittance provider WorldRemit entered Bank Negara Malaysia's (BNM) sandbox to test a solution for remote customer identification. At the time, this approach to customer identification was not permitted. After successful testing in the sandbox, BNM allowed WorldRemit to implement the solution while it concurrently issued e-KYC guidelines to permit remote customer identification for AML/KYC purposes.[27] In addition to WorldRemit, other business models that benefited from the sandbox include a digital peer-to-peer currency-exchange platform, a comparison website for insurance, credit cards, loans, and digital motor insurance.

In **Indonesia**, both the central bank, Bank of Indonesia (since 2017), and the financial services authority, the OJK (since 2018), offer regulatory sandboxes, each for firms under their remit. In the first case, the sandbox focuses on "forward looking" fintech services while the OJK sandbox focuses on fintech firms helping support financial inclusion and literacy. The Bank of Indonesia also has a dedicated fintech office since November 2016.

Other Asian jurisdictions with regulatory sandboxes include **China** (China Banking Regulatory Commission), **Sri Lanka** (Central Bank of Sri Lanka), **Singapore** (MAS), **Republic of Korea** (Financial Supervisory Service), **Philippines** (Bangko Sentral Ng Philipinas), **Taiwan, China** (Financial Supervisory Commission), **Hong Kong SAR, China** (which has two, a Fintech Supervisory Sandbox and an Insurtech Sandbox), **Japan** (Tokyo Metropolitan Government and Japan Financial Services Agency), **Thailand** (which has three, Bank of Thailand, Securities and Exchange Commission's KYC sandbox,[28] and Office of Insurance Commission) and **India** (which has four, RBI, Insurance Regulatory and Development Authority of India, State of Maharashtra, Securities and Exchange Board of India).[29]

Other Asian innovation facilitators include innovation hubs (Thailand/SEC, Singapore/MAS, Republic of Korea/ Seoul Metropolitan Government, Malaysia/BNM, Japan/Bank of Japan and Japan Financial Services Agency, Hong Kong SAR, China/HKMA and SFC) **and regtech accelerators** (Thailand/BOT, Singapore/MAS, Philippines/Bangko Sentral Ng Philipinas, Japan/Bank of Japan, India/Unique Identification Authority of India, Hong Kong SAR, China/ HKMA and SFC).[30]

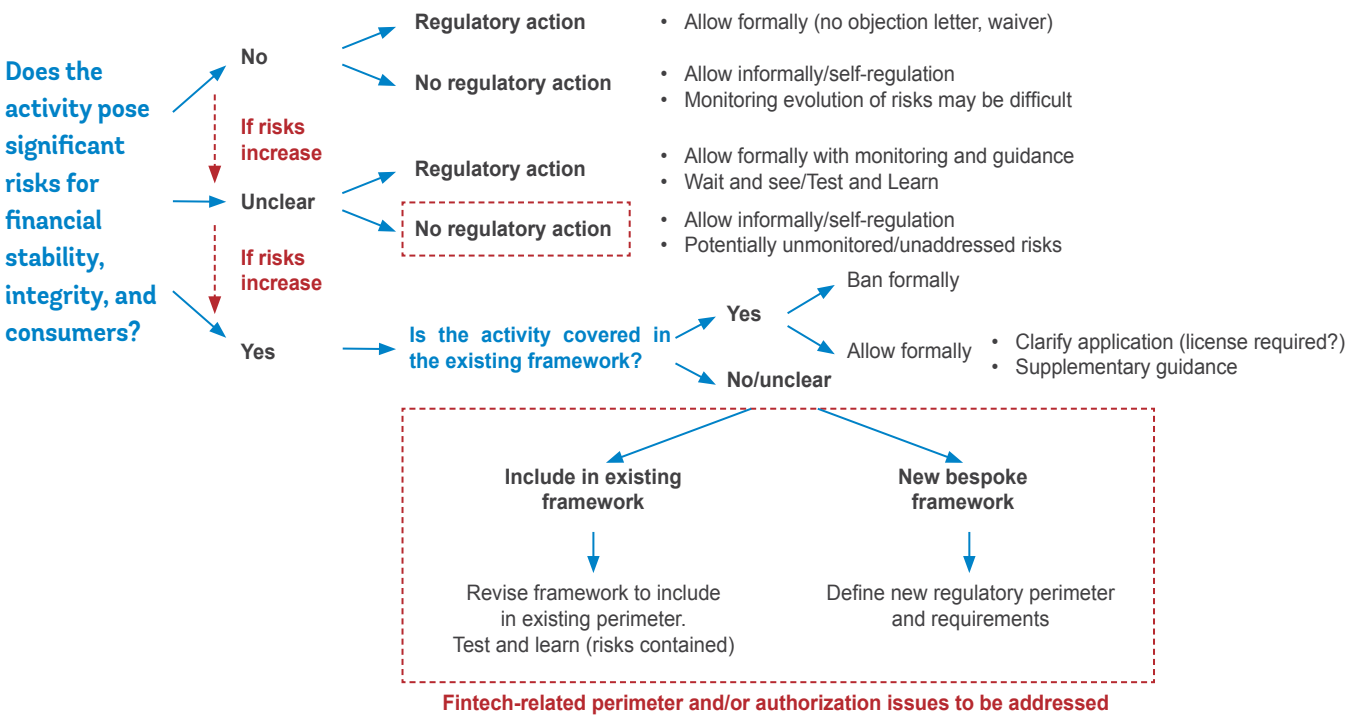
3.3 How to Regulate?

Regulatory action can cover a wide span, from marginal changes to existing regulatory settings to implementing new bespoke frameworks (figure 1). In some cases, existing frameworks are fit for purpose or need only a few amendments. This is the case, for example, of AML/CFT rules and banking regulations that apply to digital banking activities by traditional banks. In other cases, regulatory frameworks will need to be complemented by supplementary guidance (for example, Ghana's central bank issued the Guidelines for E-money Issuers and Agent Guidelines in 2015). It may also happen that

27. UNSGSA and CCAF, 2019
28. Silk Legal, "SEC Introduces KYC Sandbox".
29. See World Bank, 2020.
30. Ibid.

the existing regulations are not directly applicable to fintech activity but provide a solid basis from which to undertake the necessary changes to effectively regulate and supervise it (for example, through the introduction of new digital banking licenses in Hong Kong SAR, China, Republic of Korea, and Singapore). Finally, in some cases, new bespoke rules are required to either officially ban (for example, ICOs in China) or allow fintech activity (for example, new e-money laws in Singapore and Hong Kong SAR, China or Indonesia's regulations for lending platforms).

Figure 1. The Fintech Regulatory-Decision Tree



Source: World Bank Staff (Authors)

The policy response chosen by each country will depend on the type of fintech activity and country-specific factors. The type of risks posed by the activity and its penetration degree will be the most relevant drivers but not the only ones. Country-specific factors include the state of the market, capacity constraints, the existing financial regulatory framework, or the country's legal tradition. When the risks perceived are not high, we have observed that EMDE countries tend to allow fintech activity with no formal regulation. This may be related to the overall capacity and resource constraints that several of these countries face, the specific challenges posed by big tech firms (which offer a broader scope of services in EMDEs than in advanced economies), the often-underdeveloped state of fintech in the country, and lower competition levels in the financial service markets (FSB 2019a and 2019c).

When risks are high, EMDEs have shown a preference to either ban the activity altogether or set up new bespoke frameworks, rather than try to amend or expand existing regulations. New frameworks can result from a long consultation process and in-depth regulatory gap analysis or, alternatively, reflect a lack of capacity to conceptualize beyond a concrete business model or else respond to lobbying or political pressures. In some cases, the adaptation of the regulatory framework is not feasible or desirable and a new framework is the best response. Common law jurisdictions, being principle based, are often able to apply existing legislation to extend the regulatory perimeter to fintech activities, with just small tweaks to procedures and licensing. In civil-law countries, however, financial authorities may be constrained in regulating fintech activities by "rule-based permissions" (that is, mandates and powers) that their foundational laws confer

on them. For example, the ability of authorities to amend regulations or issue new circulars might be restricted by law, reducing the options available to the regulator (World Bank 2019). Moreover, supervisory powers issuing "no objection" formal letters, waivers, or restricted licenses are not very common in these countries.

Box 3. Regulation of E-Money Activities in Africa

The African continent is an early leader in regulating e-money. The common feature of the regulatory frameworks in Africa is that non-banks, usually mobile network operators (MNOs) or their subsidiaries, maintain liquid assets equal to the amount of money issued electronically to customers (an "e-float"). The funds are usually pooled and held by a bank or in another liquid form in the name of the MNO to ensure that customers' money is available on demand. Due to the relatively small value of individual transactions, MNOs can limit money-laundering and terrorist-financing risks by restricting the number of accounts an individual can hold and by limiting the total value of transactions over a given period, although additional measures are also often needed.[31] Initial differences in policy approaches to these services offered by non-banks have led to noticeable regional differences, which have nonetheless narrowed over time.[32]

East Africa has taken a more permissive and flexible approach. Kenya, Tanzania, and Zambia have implemented some form of Wait and See or Test and Learn before instigating regulatory reform. The Central Bank of Kenya, after a period of close monitoring, issued "letters of no objection" to two MNOs—(M-PESA and Airtel in 2007 and 2010 respectively—for their mobile money activities that set out the prudential and market conduct requirements and monitoring obligations for mobile money providers and included trust account requirements based on Trust Law. Later, in 2014 e-money licenses were issued under the National Payment Systems Regulations, setting out an authorization framework for payment service providers (PSPs), which can include non-banks. To issue e-money, PSPs are required to obtain an e-money license.[33] Tanzania has followed a similar path. The Electronic Payment Scheme Guidelines were issued in 2007 by the Bank of Tanzania (BoT), but only applied to banks and similar financial institutions. To facilitate mobile money by MNOs and other non-banks, BoT issued "no objection" letters. The 2015 National Payments Systems Act set out the legal framework for payment systems in Tanzania and clarified the mandate of its central bank, which subsequently issued Electronic Money Regulations. According to these, PSPs must be licensed under the National Payments System Act and establish a separate legal entity to be permitted to issue e-money.[34]

West Africa has taken a more cautious, reactive approach. Initially, many jurisdictions took a more rigid interpretation of relevant regulations, often prohibiting such e-money services by non-banks. Recent regulatory action was required to kick-start digital finance,[35] thereby allowing non-banks, including subsidiaries of MNOs, to issue e-money and offer limited digital financial services. Similarly, the Central Bank of West African States issued regulations in 2015 that encouraged non-banks to issue e-money, thereby enabling a whole host of West African countries to get on the mobile money band wagon. Ghana is, however, a West African outlier that took regulatory action on e-money from the start. It issued its first "Branchless Banking" guidelines in 2008, a bank-led "many to many" model that prevented exclusive partnerships but had flexible criteria for agents, including MMOs and merchants. As

31. See IMF (2019a) and Chatain et al. (2011).
32. See International Monetary Fund and World Bank. 2019.
33. The adapted requirements for an e-money license include: (i) lower initial and ongoing capital requirements than banks (KES20 million initial and ongoing for EMIs vs. KES1 billion initial and KES250 million ongoing for banks), (ii) transaction limits on e-money transactions (individual transaction limit of KES70,000 and KES1 million monthly aggregate), which do not apply to banks, (iii) restriction on EMIs in lending and investment activities, (iv) safeguarding of customer funds in a trust and diversification of the holding of the e-float, and (v) ability of the PSP to appoint agents that have a more limited remit than bank agents. A small e-money license category also exists for closed and semi-closed loop instruments, with some exemptions to the above requirements as well as a lower initial capital requirement of KES1 million.
34. Adapted requirements for e-money issuance include (i) initial and minimum ongoing capital of TZS500 million in comparison to TZS15 billion for banks, (ii) restriction of activity to payment services within transaction limits and provision of other financial services in partnership with financial institutions, (iii) safeguarding of customer funds in a trust and diversification of the holding of the e-float, (iv) ability of the PSP to appoint agents with similar requirements to bank agents, and (v) simplified KYC for lower-tiered accounts.
35. See the Guidelines for Licensing and Regulation of Payment Service Banks in Nigeria.

these guidelines provided no clear incentives for stakeholders to invest in e-money, the central bank reconsidered its approach and issued the Guidelines for E-Money Issuers in Ghana and the Agent Guidelines in 2015. The licensing provisions of the former became functional with the passage of the Payment Services and Systems Act of 2019.

3.3.1 Licensing and Regulatory Requirements

The fintech activities that pose significant risks to the financial system will likely require authorization and a supervisory license to operate. The rest might only need to be registered with or notified to the relevant supervisor. Licensing frameworks define the scope of fintech activities that are permitted and set the associated regulatory requirements for the holder with limits to the provision of the service as applicable.

- **Permitted and restricted activities:** In order to ensure that the risk profile of the fintech activity remains unchanged, entities that undertake only certain activities such as e-money issuance or crowdfunding are often restricted from undertaking other specific activities. Permitted activities are typically more narrowly defined than for banks or other financial institutions such as investment firms. For example, EMIs can usually offer payments, but not lending, while platforms offering P2P lending can provide some borrower research but may not be able to offer securities.

- **Restrictions on types of consumers:** In some cases, for example in crowdfunding and other investment-related fintech activities, the regulator may ban (or limit) the offering of a fintech activity to certain types of clients (typically retail investors) to protect them against sophisticated abusive practices.

- **Prudential rules:** These include, inter alia, initial and minimum ongoing capital and liquidity requirements for digital activities that involve intermediation of client funds, safekeeping of entrusted funds when there is only a fiduciary role such as in the case of non-bank EMIs, and adapted disclosure and regulatory compliance.

- **Governance requirements and conduct:** These rules set requirements on the composition of the management body and fit and proper criteria for shareholders and managers. In a few cases, simpler procedures may be acceptable provided they are transparent and effective, and that management is subject to fit and proper controls (that is, checks on the specific skills and knowledge related to technology applied to finance).

- **Integrity rules:** These include AML/CFT requirements adapted to digital services, including virtual and remote account opening without the need to present physical identity documents. These adapted AML/CFT rules—often predicated on account, transaction, and balance limits to ensure low-risk profiles of clients—are supported by recent guidance from the Financial Action Task Force on digital ID and the use of a risk-based approach to CDD with regard to electronic and digital payment options.[36]

- **Agents:** Financial service institutions may wish to use agents to broaden their reach and penetrate rural and other less densely populated areas. Depending on the type of activity, the agents may (or may not) be authorized and. if permitted, subject to certain restrictions in their activities and geographical locations. These restrictions and processes should be adapted to the risk profiles of the agents' activities.

---

33. The adapted requirements for an e-money license include: (i) lower initial and ongoing capital requirements than banks (KES20 million initial and ongoing for EMIs vs. KES1 billion initial and KES250 million ongoing for banks), (ii) transaction limits on e-money transactions (individual transaction limit of KES70,000 and KES1 million monthly aggregate), which do not apply to banks, (iii) restriction on EMIs in lending and investment activities, (iv) safeguarding of customer funds in a trust and diversification of the holding of the e-float, and (v) ability of the PSP to appoint agents that have a more limited remit than bank agents. A small e-money license category also exists for closed and semi-closed loop instruments, with some exemptions to the above requirements as well as a lower initial capital requirement of KES1 million.
34. Adapted requirements for e-money issuance include (i) initial and minimum ongoing capital of TZS500 million in comparison to TZS15 billion for banks, (ii) restriction of activity to payment services within transaction limits and provision of other financial services in partnership with financial institutions, (iii) safeguarding of customer funds in a trust and diversification of the holding of the e-float, (iv) ability of the PSP to appoint agents with similar requirements to bank agents, and (v) simplified KYC for lower-tiered accounts.
35. See the Guidelines for Licensing and Regulation of Payment Service Banks in Nigeria.
36. Under this approach, the activity is the subject of regulation by the licensing framework, regardless of the legal character of entity/ institution that is offering the services.

- **Data protection:** These provisions are gaining increasing regulatory relevance in the context of fintech. They can often be found in specific licensing frameworks (for example, in e-money frameworks), general guidelines for financial service entities, and in national data protection laws. In the latter case, a data protection authority usually has joint jurisdiction over the financial service entities. The regulation of data-protection risks, however, must be balanced, as data policies that are too stringent could prevent beneficial innovations such as inclusive credit based on data analytics, impose competitive disadvantages to those that collect the data, or prevent customers and businesses from sharing information to obtaining loans, insurance, or other financial services (Petralia et al.,2019). Further, financial authorities need to consider the interaction of any financial service data protection provisions they impose with broader national data-protection frameworks (CEMLA, 2019). Lastly, data localization laws—that is the restriction of data flows across borders—have in recent years found favor with several EMDEs (for example, China, India, Nigeria, and Vietnam). These restrictions vary across jurisdictions, but generally capture some of the activities in which big tech firms engage, such as cloud storage and/or data processing, and could thus have an important effect in stymieing competitive pressure from big tech firms in financial services (FSB 2020b).

Digital banking services involving deposit taking are often permitted by a (sometimes temporary) extension of the banking licensing framework. Some jurisdictions have opted for a phased licensing process through which new entrants start operations with limited activities and finally become fully licensed banks. Regulators mainly focus on facilitating the authorization process for deposit-taking institutions with a technology-intensive business model, like Australia's temporary restricted license for authorized deposit-taking institutions for fintech startups or the U.K.'s sequenced licensing option for banks. In Asia, authorities are starting to issue specific licensing frameworks for digital-only banks (for example, virtual banks in Hong Kong SAR, China; internet-only banks in Republic of Korea and Taiwan, China, digital banks in Singapore), which have restrictions on physical presence and a focus on financial inclusion while leaving in place the fundamental requirements for banks (that is, AML/CFT and consumer protection rules, risk management, and certain prudential requirements like minimum capital).[37] Other examples of new licenses are those for payment banks in India and mobile financial service providers in Bangladesh.

Given their rapid expansion and key role in promoting digital financial services and inclusion, many jurisdictions are actively adopting a risk-proportionate approach to bring digital payments and e-money services into the regulatory perimeter (box 3).[38] Firms engaged in these activities have regulatory requirements as undertakers of the payment (often from a virtual account) and are usually required to have a license with prudential and conduct requirements that are proportional to their risks to safeguard customer funds and integrity (see also section 5.2). Account Information Service Providers, who do not transmit customer funds, are frequently subject to a registration or notification requirement and much lighter prudential, operational, and security obligations, given the lower risks involved.

Due to their enormous potential in helping improve access to finance for small and medium enterprises (SME), countries are increasingly seeking to cover crowdfunding platforms in their legal and regulatory frameworks. These P2P lending platforms help connect investors with borrowers or corporates seeking to raise funds by selling equity or debt. Some countries have enacted a single framework to encompass both securities-based crowdfunding and lending crowdfunding (for example, Mexico).[39] Other jurisdictions have opted for separate regimes (Brazil), a model that seems more prevalent in countries with a sector-based supervisory model (particularly common in Africa and Latin America), although separate regimes exist in countries with a unified supervisor (for example, Indonesia). Box 4 below develops in further detail the main considerations regarding the regulation of securities-based crowdfunding platforms (although differences from regulation for lending platforms are generally small).

37. See Kerse and Jenik, 2020 (blog entry here).
38. See Dias and Staschen 2018.
39. In Mexico, entities providing these services must be authorized as "Financial Technology Institutions".

Box 4. Regulation of Securities-Based Crowdfunding Platforms

No regulatory model can be considered as a best practice (as yet). The authorities' understanding of the risks posed by crowdfunding business is still evolving. However, some key features and lessons can be extracted from the frameworks enacted by some advanced economies and EMDEs.

The operators of platforms are usually subject to licensing, often involving a specialized license that bans the undertaking of any other activity. In addition to the holders of these specialized licenses, many countries allow certain types of intermediaries to operate the platforms (for example, recognized exchanges, broker-dealers). While initially not all specialized licenses for securities-based crowdfunding platforms imposed capital requirements, there is a growing trend towards imposition of minimum (low) capital requirements, which in some cases vary with the total volume of funds raised. Platform operators are required to comply with AML regulations and most frameworks require certain basic organizational requirements, including in relation to risk management. They must abide by key business conduct obligations such as (i) ensure that the companies and investors do not exceed the fund raising and investment limits set forth by regulations, (ii) keep investors' money segregated, (iii) conduct basic due diligence of the companies raising funds on the platforms and the information they provide, (iv) conduct basic KYC procedures on investors and provide them with information about the progress of the offerings as appropriate to the instrument; and (v) provide sufficient information to users about the platform's role, the services provided, and any fees that apply.

The users of the platforms are also subject to light disclosure and (sometimes) governance requirements. The frameworks usually target domestic companies, in some cases focusing on SMEs and/or companies that have not had public offerings or are not listed. Disclosure requirements are lighter than those applicable under the traditional public offering regime. Having a prospectus is usually not mandatory, but some basic information on the business of the fund-raising company or the project that it is seeking to fund is required. In some countries, fund raisers are required to present their financial statements, but this information is not necessarily reviewed ex-ante by the regulator.[40] Periodic and ongoing disclosure requirements are limited. Firms must inform on progress in the offering in a few cases, for example in connection with certain adverse events. Corporate governance requirements are rare, but some basic rules generally apply as per corporate law.

Most countries are imposing limits on the amount of funds raised through these platforms to compensate for lighter requirements. Several countries are capping the amount of money that firms can raise through securities' crowdfunding platforms, with relatively low caps. Some countries are imposing limits on the amount that investors can invest in a single firm or project. These investment limits tend to be proportional to the investor's income and hence apply mostly to retail investors, although several countries are considering increasing them. While positive from an access to finance perspective, these increases could jeopardize the protection of retail investors if they are not well calibrated. Further, the more these limits are expanded, the fewer firms may use public capital markets to raise funds, with potential implications for the depth of these key markets.

3.4 Linkages: Prudential and Competition Considerations

The emergence of fintech may force fundamental changes in market structure and therefore in the approach to competition policy, including through increased participation by financial service authorities. Digital markets have certain structural characteristics that may make them less contestable and more prone to tipping in favor of a single dominant firm.[41] Indeed, there is growing evidence that greater access to and use of technology and Big Data by fintech

40. For issuances above a certain size threshold, a few countries require that these be certified or audited.
41. Network effects, sunk costs, economies of scale and scope, and other entry barriers.

providers, especially big tech firms (including as service providers to financial institutions), facilitates price discrimination and other uncompetitive behavior, including limiting access to communication and payments infrastructures, restricting the use of agents through exclusive contracts, keeping data in silos, and refusing to interoperate (Carletti et al. 2020). Although *ex post* antitrust measures, such as sanctions imposed on financial service market players for anticompetitive behavior,[42] are usually taken by competition authorities, in certain countries financial regulators have supporting competition as part of their mandates and can implement certain *ex ante* regulations to ensure the contestability of the market and a level playing field with regard to data, technologies, and infrastructure. Examples include providing non-banks access to payments infrastructure (Mexico), giving non-bank credit providers access to credit registries (China), or facilitating access to data and the ability to initiate transactions through open banking (Brazil).

Many countries are implementing open banking initiatives to promote competition. Latin America regulators are at the forefront among EMDEs, which in part may be explained by relatively high rates of bancarization and a comparatively high percentage of financial sector regulators (36 percent) having a statutory mandate to promote competition (World Bank and Cambridge Centre for Alternative Finance, 2019).[43] Article 76 of Mexico's Fintech Law, introduced in 2018 high-level provisions for a mandatory open banking scheme and the details of the scheme were then set out in a secondary regulation issued by the Bank supervisor and the central bank of Mexico in 2020. The central bank of Brazil issued a resolution in May 2020[44] implementing an open banking scheme that is mandatory for the largest banks, prudential conglomerates, and payment institutions.[45] Although the central bank of Brazil does not have an explicit competition mandate, it has adopted competition as a strategic goal, and according to Art. 3, Section II of the resolution, one objective of its open banking scheme is to promotion of competition.[46]

There is an ongoing debate about whether financial regulation for fintech should aim at preserving the level playing field and if so if this would be best attained through an activities-based approach. Financial regulations may limit the entry of fintech firms, indirectly favor incumbents, or advantage a certain type of market actor; for example by allowing only one type of institution to undertake a particular activity, not regulating certain actors, or imposing requirements that are not risk-proportionate (Vives 2019). Given this, the need to take a closer look at regulations and seek to make them as competition friendly as possible seems pertinent. Yet, this should not happen at the expense of the fulfilment of the core surveillance and oversight mandates. Indeed, some regulatory policies that aim to increase competition (for example, open banking) might be shifting concentration from one group of entities to another, for example, from financial incumbents to big tech firms, with potential implications for stability. As stated by Restoy (2021): *"Helping to achieve a level playing field in the financial sector is a desired outcome of the regulatory framework…only when higher-priority policy objectives are ensured."*

The expansion of big tech firms into financial services is poised to create fundamental changes in the structure of the sector, especially in EMDEs where such expansion is particularly rapid and broad-based. Big tech firms are playing an increasingly prominent role in the financial system as providers of financial services, where they can leverage their large existing customer base to achieve scale rapidly. They are already enjoying a dominant position in several countries across a range of financial services such as payments, lending, insurance, and investment management. Mobile payment platforms, including those integrated into social networks, have seen rapid uptake by hundreds of millions of users across many jurisdictions. The range of financial services provided by big tech firms is also greater in EMDEs than that in advanced economies. This is particularly true in some jurisdictions in Asia—Bangladesh (bKash), China (Alibaba, Tencent, and Baidu) and Indonesia (GO-JEK)—where some big tech firms offer a suite of financial services. Credit provision by big tech firms has shown accelerated growth in countries such as China and Indonesia, bringing a new set of challenges to regulators and supervisors (FSB 2019a; IMF-WB 2019, Crisanto and Ehrentraud 2021).

42. European Commission, 'Antitrust: Commission Opens Investigation into Apple Practices Regarding Apple Pay'.
43. A statutory mandate to promote competition is not required to implement open banking.
44. Joint Resolution No. 1 of May 4, 2020 providing for the implementation of Open Banking.
45. The scheme came into force in June 2020 and will be fully implemented in December 2021.
46. The entity responsible for the development of technical standards related to open banking initiatives may vary across jurisdictions. For example, in Mexico, technical standards are articulated by the financial sector regulator and in Brazil, a convention drafted by industry stakeholders is responsible for the standards, though they are subject to regulatory approval by the central bank (Plaitakis and Stachen 2020). In the United Kingdom, a dedicated government entity oversees the implementation of open banking, including the development of API standards.

While an activities-based approach generally works well to preserve integrity and protect consumers, with the presence of big tech firms, stability objectives may be best achieved by using an entities-based approach.[47] Big tech firms must hold licenses to offer services such as payments, wealth management, or credit underwriting and, as such, they are bound by AML/CFT and consumer-protection rules.[48] On the prudential side, there is now a debate on whether big tech firms should be regulated institutions. The Bank of International Settlements (BIS) considers that the entry of big tech firms presents *"new and complex trade-offs between financial stability, competition, and data protection"* that need to be addressed. In a recent brief, the FSI observes that risks arising from the development of big tech activities in finance *"may not be fully captured by the regulatory approach…,which is geared towards individual entities or specific activities and not the risks that are created by substantive interlinkages within big tech groups and their role as critical service providers for financial institutions."*[49] The two main arguments in favor of bringing big tech firms into the regulatory perimeter are thus (i) to address operational resilience concerns in case big tech operations reach a systemic importance, and (ii) to mitigate the risks that big tech firms will reach a dominant position from which they could adopt anti-competitive practices and force out most other competitors to then impose monopolistic pricing in the long term. As stated by Padilla 2020, *"…while big tech firms may spur much-needed competition in the short term, [they] may also increase financial instability and lead to even more concentrated credit markets in the long-term. Importantly, traditional banks may be forced to transform into "narrow banks", limited to funding the loans originated and distributed by the big tech firms."*

47. See Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy (Market Structure note) for the argument that similar activities and similar risks should be treated similarly, regardless of the market participant, underlying technology, or method by which the service is provided, and Restoy 2021 for the argument that regulations should be a mix of activity and entity-based rules, with differences in regulatory requirements justified on the basis of higher-priority policy objectives.
48. See Carstens, A., Public Policy for Big Techs in finance. BIS, Introductory Remarks, January 2021 and FSI brief no. 12 (2021).
49. Ibid.

4. Specific Supervisory Challenges

An effective supervisory function for fintech activities is as essential as an appropriate regulatory regime. Regulation and supervision are two sides of the same coin. The unprecedented acceleration of technological developments and their vast application across the financial system create specific supervisory challenges. The growing number of emerging digital technologies and actors involved (from small new third-party providers to big tech firms) has put the spotlight on the supervisor's responsibility to appreciate the fintech landscape and monitor new ways by which risks and vulnerabilities can materialize and spread across the system. New technologies (machine learning, artificial intelligence, cloud computing, APIs) accelerate the process of bringing products and services to the market, calling for swift supervisory action when required. Others, such as the distributed ledger (DLT) allow for a degree of decentralization that calls into question classic notions of liability, responsibility, and transaction reversibility. The volume of data involved has expanded exponentially in the last few years and supervisors must be able to process and analyze to monitor and assess risks and vulnerabilities. Only by having a good understanding of how these technologies operate (their business model and main technical constraints and specificities) will authorities have the expertise to properly regulate and supervise fintech.

4.1 Devising an Effective Supervisory Function for Fintech Activities

Without adequate supervision, the main public policy objectives of preserving financial stability and integrity while protecting consumers and investors would not be achieved. The supervisory framework for fintech should be well-designed to respond to the risks inherent in the fintech activities, flexible enough to adapt to changes driven by the introduction of new products/services, distribution channels and other characteristics of fintech's high dynamism. The framework should also embed proportionality, so that the supervisory response is graduated according to the level of risk posed by an activity.

Countries are continuously reassessing the appropriateness of their frameworks to account for the rapidly evolving fintech phenomenon and its impact over the financial sector. No country has instituted a single institutional model to supervise fintech activities. Rather, supervisory responsibilities for fintech tend to follow frameworks and mandates in place for financial sector supervision, although in some countries three is a debate on whether existing frameworks and approaches remain appropriate or whether adaptation and change is needed (IMF 2020).[50] New responsibilities are being allocated to existing authorities. Since some services previously provided by established financial institutions are now also provided by non-financial corporates and startups, questions arise as to how the regulatory perimeter should be set and which authority should supervise.

Each authority must determine the best supervisory approach for their jurisdiction, possibly looking at the global standards for sound supervision of traditional activities for inspiration. Authorities will need to adjust and prioritize their oversight and surveillance function for fintech activities based on (potential) risks, rates of adoption, players involved,

50. The division of responsibilities typically falls under one of the three common supervisory structures: (i) a twin-peaks model with a prudential and conduct supervisor (for example, U.K. and France); (ii) a sectoral approach, where responsibilities are divided along industry lines (for example, banking, insurance, and capital markets—for example, in Hong Kong SAR, China, Kenya, and U.S.); or (iii) an approach based on a single, integrated supervisory authority (for example, Singapore, Switzerland).

or local market conditions. For risks impacting regulated firms (banks, insurers, securities firms, etc.), they can also look at global standards to understand the ways in which fintech impacts incumbents and how their supervision should be adjusted (for example, the Basel Core Principles for Effective Banking Supervision provide a good reference to assess impact of fintech over banks. See box 5 below).

Box 5. Using Global Standards as a Proxy Benchmark

The Basel Core Principles for effective banking supervision (BCP) set minimum standards for sound prudential regulation and supervision of banks in core areas. While fintech developments and related risks for banks are not explicitly mentioned in the BCP text, many of the 29 Core Principles (CP) are flexible to accommodate for an assessment of fintech-related risks for the banking sector and its supervision in a given country. Below are a few examples of relevant CPs and related burning questions supervisors could consider.

CP #7 deals with *major acquisitions* and requires supervisors to impose prudential conditions on major acquisitions or investments by a bank and assess any impact. For banks acquiring significant stakes in fintech firms (for example, through outright acquisition, joint ventures, partnerships, or shareholding interests in fintech companies), supervisors should assess whether such acquisitions could expose the banks to undue risks or hinder their effective supervision. Other relevant questions include: (i) What is the impact of foreign operations of domestic fintech firms on the acquiring bank and vice versa? or (ii) How should the supervisor determine that the bank has adequate financial, managerial, and organizational resources to handle the acquisition of or investment in fintech company?

CP #25 is about *operational risk* and recommends that the supervisor determine that banks have an adequate operational risk-management framework that considers their risk appetite and risk profile. Also, outsourcing policies and processes require the bank to have comprehensive contracts with a clear allocation of responsibilities between the outsourcees and the bank. As explained in section 2, fintech exacerbates operational risk (OR) for different reasons. Considering the interdependencies between market players and the excessive reliance on fintech third-party providers (with limited experience in managing IT risks and cyber risks), to what extent can a supervisor ensure that outsourcing arrangements are sound? Did the supervisor set out clear cybersecurity standards for both banks and for any other fintech providers under its purview?

CP #29 on *AML/CFT* requires banks to have adequate policies and processes to prevent being used for criminal activities. As seen in section 2, these risks can be exacerbated in a financial sector with a significant digital footprint. Hence supervisors should determine what AML/CFT measures supervised entities have taken to mitigate integrity risks arising from fintech developments. Similarly, supervisory authorities should determine whether there is a need to set AML/CFT requirements with respect to non-face-to-face money transfer and crowdfunding platforms, internet, mobile banking, and virtual assets (crypto-currencies). Similarly, AML/CFT control mechanisms to supervise fintech inherent risk factors (anonymity, traceability, functionality) might be required.

4.2 Addressing Specific Risks Raised by Fintech Developments

As discussed in section 2, risks arising from fintech are hardly new to supervisors but some can be considerably exacerbated or may build up at higher speeds than for traditional financial activities, calling for specific regulation, as discussed in section 3, and supervision, as discussed below.

4.2.1 Cyber Risks

Cyber threats are bound to increase in an increasingly fintech dominated financial sector, calling for prompt and timely supervisory action. In October 2016, in response to several high-profile cyber threats, the G7 issued the *Fundamental Elements of Cybersecurity* for the Financial Sector.[51] It subsequently published a high-level assessment framework, with five components[52] for effective assessments of cybersecurity for use in regulatory examinations. That same year CPMI/IOSCO issued guidance on cyber resilience for financial market infrastructures.[53] In 2017, the FSB published a stock take on cybersecurity regulations, guidance, and supervisory practices emphasizing that effective cybersecurity requires a strategic, forward-looking, fluid, and proactive approach (FSB 2017b). In 2018, the Basel Committee on Banking Supervision (BCBS) documented a range of cyber-resilience practices in banking. Finally, in 2020, the FSB issued a toolkit (FSB 2020c)[54] that includes 49 practices for effective cyber-incident response and recovery across seven components: (i) governance, (ii) planning and preparation, (iii) analysis, (iv) mitigation, (v) restoration and recovery, (vi) coordination and communication, and (vii) improvement.

A wide range of supervisory practices to counter cyber risks exist, with EMDE supervisors catching up. Enhancing cyber-incident response and recovery at organizations is an important point of focus for national authorities. They are in a unique position to gain insights on effective cyber-incident response and recovery in financial institutions from their supervisory work and their observations across multiple organizations can help suggest areas for enhancement.[55] Based on the international guidance listed above, supervisory requirements to mitigate cyber risks typically consist of: (i) a documented cybersecurity program or policy aligned with CPMI/IOSCO guidance; (ii) identification of critical information assets; (iii) testing; (iv) cyber-event reporting; (v) cyber-threat intelligence sharing; (vi) documented security capabilities of third-party service providers; and sometimes (vii) security certification of information security professionals.[56] Increasingly, supervisors use a threat-informed or intelligence-led testing framework, in which cyberattacks are simulated to test cybersecurity.[57] Banking supervisors also explicitly refer to external standards issued by agencies specializing in IT security with whom they increasingly cooperate. In France for example, the ACPR, the Prudential Supervision and Resolution Authority, and ANSSI (National Agency for the Security of Information Systems) announced in January 2018 the signing of an agreement providing for a regular exchange of information on incidents affecting information-systems security. Further, supervisors integrate cybersecurity risks in the performance of their onsite control missions. The ACPR has acquired specialized teams in this area and conducts, among other things, penetration tests to assess the robustness of banks' systems (Castanier and Roussely, 2018). Many supervisors also ask for external cybersecurity assessors to undertake cybersecurity assessments and provide reports to supervisors and the financial institution—the cost being borne by the financial institution.

4.2.2 Increased Reliance on Third-Parties

As outsourcing arrangements are becoming more prevalent (and potentially systemic), supervisors are developing a more structured approach to address the increasing complexity. One principle that supervisors follow with outsourcing arrangements is proportionality.[58] The European Banking Authority puts it this way: *"Financial institutions and payment institutions should take into account the complexity of the outsourced functions, the risks arising from the outsourcing arrangement, the criticality or importance of the outsourced function, and the potential impact of the outsourcing on the*

51. The seven elements are: (i) strategy and framework, (ii) governance; (iii) risk and control assessments; (iv) monitoring response; (v) recovery; (vi) information sharing; and (vii) continuous learning.
52. The five components are: objectives, methodology, tools, reporting and fairness of assessments.
53. "Guidance on Cyber Resilience for Financial Market Infrastructures." CPMI-IOSCO, 2016.
54. Effective Practices for Cyber-Incident Response and Recovery: Final report, October 2020.
55. FSB: https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/
56. See also the G7 Fundamental Elements of Cybersecurity for the Financial Sector and the FSB 2018 "Cyber Lexicon", which provides a common terminology to facilitate work on cyber resilience and security.
57. BoE 2016, CBEST Intelligence-Based Testing, ECB 2018, TIBER-EU Framework – How to Implement te European Framework for Threat-Intelligence-based Ethical Red Teaming.
58. EBA 2019: *"The proportionality principle aims to ensure that governance arrangements, including those related to outsourcing, are consistent with the individual risk profile, the nature and business model of the institution or payment institution, and the scale and complexity of their activities so that the objectives of the regulatory requirements are effectively achieved."*

continuity of their activities". The United Kingdom[59] and Brazil[60] also use a balanced approach, in which critical services or functions require prior authorization and requirements on, inter alia, data security, data protection and privacy, auditability, due diligence of the provider, contingency plans, and reporting obligations. Cloud-based infrastructure, in particular, raises unique concerns relating to outsourcing practices. Institutions may lose physical access to the stored data and its processing, which are controlled by computing service providers (CSPs). As stated by the Toronto Center: *"Using the cloud increases the number of potential points of failure, while the location and conditions of data are not necessarily known or determined by the financial institution. CSPs use geographically dispersed infrastructure with regional or global distribution, and they service both financial and non-financial sectors, challenging traditional audit and risk-assessment methods."*[61]

While some EMDE jurisdictions are cautious in relation to cloud-computing practices, others impose no minimum requirements. In some countries, supervisors have resorted to Test and Learn approaches to allow incumbents step into fintech options while ensuring a close monitoring and a sound supervisory role (box 6). Countries such as Australia, Brazil, Canada, and Colombia have issued specific guidance or supervisory expectations, either as a standalone document or as part of a broader regulation (Dias, 2020). Some EMDEs have imposed data localization and domestic data replication requirements or outright prohibition, or limitations, of cloud computing.[62] But several low-income jurisdictions have not specified minimum requirements for third-party providers at all, which may introduce significant risk.[63]

Box 6. Community Cloud Computing for Rural Banks in Philippines

In 2019, as part of BSP's Test-and Learn approach to financial innovation, a rural bank requested a pilot to move its core banking software to a community (international) cloud provider.[64] The bank wanted to reduce costs, increase data security, and focus on its mission of financial inclusion. BSP also saw the potential to streamline its risk-based supervision for other rural banks were they to join the same community cloud.

The supervisory process included a thorough review of documentation, including responses to questionnaires, and an external security report. The 18-month pilot, during which supervisor and supervised entity collaborated continuously, led to a better understanding of the risks, challenges, and benefits associated with the technological change and resulted in a streamlining of the approval process for similar applications.

4.2.3 Data Protection

Data protection is among the most sensitive issues arising from the fintech revolution and constitutes a major challenge for supervisory agencies. A fundamental right to privacy can be seriously threatened by the massive capture and mining of behavioral data by certain fintech firms. Massive breaches of consumer data in recent years have left consumers vulnerable to identity theft and exploitation. In 2017, a U.S. credit reporting and fintech company experienced a data breach compromising the social security numbers and personal financial information of over 146 million clients. As mentioned in section 2, data protection provisions are increasingly found in licensing frameworks (for example, in e-money and payments) and in general guidelines for financial service entities or, alternatively, in national data protection laws, in which case a data protection authority may have joint jurisdiction with financial supervisors over financial service entities. Authorities are increasingly paying attention to disclosure of the types of data used by financial institutions and on

59. https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-cloud-and-other-third-party-it
60. https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf
61. Toronto Center: Cloud Computing, Issues for Supervisors, November 2020.
62. https://www.cgap.org/blog/regulators-friend-or-foe-cloud-computing-financial-inclusion
63. FTESF p. 19; see also SPIFD annex 2 p. 44 for supervisory regimes for third-party service by country.
64. The 2013 BSP IT Risk Management Guidelines from Bangko Sentral ng Pilipinas (BSP) allowed cloud computing, but only for non-core banking operations and with limited options. For a full coverage of this case study see "Cloud Computing for Financial Inclusion: Lessons from the Philippines," CGAP 2019.

measures to help consumers understand how a financial institution is using their data and to be able to grant or withdraw permission for personal data to be used. Constraints on sending data across national borders are also increasingly applied (Toronto Centre, 2019).

4.3 Overcoming Supervisory Capacity Constraints

Implementing a policy and supervisory response to fintech can be particularly challenging for EMDE countries due to capacity constraints and with competing policy priorities. Financial supervision seems to be at a turning point with important strategic decisions to be made to monitor and manage risks properly, including sending the right signal to supervised entities about risk tolerance. In many low-income countries, supervisors are just starting to understand how the new technologies are impacting the financial sector and where to hire or how to train staff with the new and rare skills that are required. The use of regtech and suptech can be a key enabler in this endeavor. Engaging early in the "suptech journey" can send a clear and positive signal to market players that the authorities are willing to accompany an evolving sector so that supervisory methods can be adapted, remain relevant and, consequently, the financial system can remain safe and trustworthy.[65]

Fintech supervisory resources generally consist of a core group supported by an expert network, but other less centralized models also exist. The advantages of having a centralized, dedicated fintech core team include increasing specialization and expertise. Core team members are also generally involved in assisting fintech firms with license issues and provide guidance throughout the process, including in innovation facilitators. On the other hand, the distribution of responsibilities for fintech among routine supervision units may help spread expertise across the agency and draw from a broader knowledge of the financial sector and risk-management disciplines (IMF, 2019). An intermediate option is to set up internal working groups that analyze the risks involved, the level of detail required by examinations, whether dedicated teams would be appropriate or not, and what specific expertise and techniques are required (for example, analytical and audit procedures).

Supervisory agencies should regularly assess staff skills and address training gaps to underpin an effective oversight function.[66] Most authorities in advanced economies have made changes to enhance their supervisory capacity along these lines (IMF and WB, 2019) but EMDEs' efforts to build up IT examination capacity seems to be progressing at a much lower pace. One starting point is to conduct a skills-gap assessment to map out essential skills that are lacking. To fill in the gap, supervisors can launch fintech training programs and/or adjust their hiring programs. A variety of training opportunities are available to EMDE supervisors, including capacity building by the World Bank, FSI, and Toronto Centre. Alternatively, to avoid relying on hiring scarce specialists, in some countries supervisors require fintech companies to obtain and directly submit third-party certifications.

Narrowing the knowledge and skills gap can be accelerated through collaboration with industry. Innovation facilitators, including regulatory sandboxes, accelerators, and innovation hubs, provide excellent learning opportunities for supervisors. They may help to greater understand innovative business models, allow supervisors to explore the risks associated with these activities, and determine what data is needed to effectively supervise the entities, while explicitly addressing the risk of regulatory capture. Supervisors can also learn from each other's experiences with such facilitators.[67] One example is HKMA's Cybersecurity Fortification Initiative, a professional development program, jointly developed with

65. Denis Beau: Financial Regulation and Supervision Issues raised by the Impact of Tech Firms on Financial Services, BIS, Central Bank Speeches, Janvier 30, 2019.
66. BCBS 2018 Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors. Consideration 7—Resources: assess current staffing and training programs.
67. SPIFD Consideration 10.

industry and academia, that seeks to increase the supply of qualified cybersecurity professionals in Hong Kong SAR, China by developing certification and training.[68] Japan, the United Kingdom, and Singapore offer additional examples.[69]

New specialists may be needed in areas such as IT security, the assessment of outsourcing contracts and service-level agreements (SLAs). Hiring programs for new staff should expand into new skill areas required for effective supervision. These include (i) distributed ledger technology (DLT), to better understand use cases and associated risks; (ii) data science, to exploit the analytical capabilities of Big Data; and (iii) statisticians and mathematicians, to help understand the modeling used by financial institutions. One area particularly challenging is the oversight of issuers of cryptocurrency-related services. Since it may be difficult to build this capacity in-house, authorities should have the flexibility to hire experts from the private sector.[70]

4.4 Increasing Cooperation

4.4.1 Cooperation at the Domestic Level

An effective supervision of fintech activities can be facilitated by coordination and information-sharing between domestic authorities. Fintech activities may fall in the regulatory perimeter of multiple agencies but[71] only a few jurisdictions have a formal body in charge of coordinating fintech policies, such as South Africa's Inter-Regulatory Fintech Working Group and the HKMA Fintech Supervisory Sandbox.[72] Collaboration mechanisms may be formalized through memoranda of understanding (MoUs) to cover cross-cutting issues such as AML/CFT or consumer protection. A good example of cross-sectoral cooperation is found in Bangladesh, where the central bank and the Telecommunications Regulatory Commission are part of a multi-stakeholder consultative committee on USSD communications, which is an essential upstream input for mobile money services (Plaitakis et al., 2016). The national or federal government might get involved in these MoUs when the impact transcends the financial sector, for example in relation to digital ID, data privacy, or cybersecurity. This work is often done, under ministerial responsibility, by a sub-committee, taskforce, or working group (for example, Thailand's Three Regulator Steering Committee). Their mandates are to study and understand fintech firms and business models, assess opportunities and risks, and investigate the necessary changes to align regulation and supervision with how the market is evolving. In some jurisdictions, supervisors engage with industry to speed up the analysis and adoption of innovations, including through innovation accelerators.

Involving the industry in fintech coordination efforts in cybersecurity, payments and securities is becoming frequent. In Brazil, there are various private/public working groups, involving, inter alia, the Payments Association, the Association of Digital Credit, and the Association of Fintechs. South Africa's Intergovernmental Fintech Working Group is another example of how engaging with the industry to develop a deeper understanding of the fintech business models can help identify an appropriate regulatory response. In Indonesia, the OJK has set up the Fintech Advisory Forum, which brings together several agencies and ministries. In France, the Fintech Forum is an example of "watch, dialogue, and proposition" between industry, experts, and public authorities. It meets twice a year and thus far has discussed proportionality in licensing

68. In 2016, the Hong Kong Monetary Authority (HKMA) established the so-called Fintech Career Acceleration Scheme to expand the fintech talent pool. This program provides individuals at the start of their careers with the opportunity to work on fintech, both in-house at the HKMA or in partner institutions: https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/talent-development/
69. BCBS, 2018. Cyber-resilience: Range of Practices.
70. These challenges are already present in advanced economies. FSI 2017 reports that medium and small institutions in the U.S. were examined by staff with little or no IT training; more generally, hiring and retention of IT security personnel in the public sector was found to be difficult.
71. These agencies may include the Treasury, Prudential Authority, Central Bank, Financial Sector Conduct Authority, Financial Intelligence Center, National Credit Regulator, Stock Exchange authority.
72. The three main financial regulators in Hong Kong SAR, China (Monetary Authority, Securities and Futures Commission, and Insurance Authority) have a single point of entry regulatory sandbox. If a firm wants to test a cross-sector fintech product, it can apply to the sandbox it considers most relevant. The regulator will act as the primary point of contact and assist in liaising with the other regulators for the firm to access the sandboxes (more details here: Hong Kong Monetary Authority - Fintech Supervisory Sandbox (FSS) (hkma.gov.hk)).

and supervision, data usage, and customer identification. Cooperation and information-sharing around cybersecurity is particularly urgent. Examples include (i) South Africa's National Cybersecurity Hub, which coordinates cybersecurity response activities and facilitates information and technology sharing; (ii) Kenya's Safaricom-led mobile money and fraud risks forum and (iii) The Nigeria Electronic Fraud Forum, led by the Central Bank of Nigeria, to strengthen cybersecurity of the country's e-payment platforms. Collaboration on cyber-risk matters requires a high level of trust and confidentiality to foster open discussions on sensitive topics. For this reason, they might be led by the industry, for example by the fraud and security community.[73] Examples are the South African Banking Risk Information Center (SABRIC) or GSMA's Fraud and Security Group in the international context.[74]

4.4.2 Cooperation at the International Level

International supervisory cooperation on fintech matters is well underway, both in bilateral and in multilateral contexts, but further guidance is welcome, including on suptech standards (IMF-World Bank, 2019).[75] Aware of the cross-border nature of fintech developments (crypto-assets, cross-border payments or cloud service providers), most countries have shared information on policy responses to international organizations or other authorities. Such cooperation facilitates knowledge transfer and sharing of good practices across countries. International cooperation partners include host supervisors; regional supervisory bodies, standard-setting bodies such as BCBS, CPMI, International and Regional Financial Institutions including the IMF and World Bank, and the recently created BIS Innovation Hub. Several EMDEs and advanced economies have signed Fintech Cooperation Agreements between the innovation units of regulatory agencies and projects such as Jasper (Canada-Singapore cross-border central bank settlement based on digital-ledger technology) demonstrate the successful completion of joint fintech proofs-of-concept. The MoU signed in June 2020 between members of the Canadian Securities Administrators (CSA) and the Financial Supervisory Commission of Taiwan, China (FSC) offers another example of bilateral cross-border cooperation. As cooperation on supervision of cross-border fintech firms increases, supervisory colleges will need to update their home-host agreements.

Initiatives to foster cooperation to agree on standards to develop suptech solutions that are compatible across countries are particularly necessary and valuable. One example is the Datastack proposal (di Castri et al., 2020), which proposed a new shared data architecture for supervisors as well as the wider financial ecosystem. A prototype developed in Nigeria focuses on payment systems oversight and financial inclusion and also covers consumer protection.[76] International hackathons and techsprints can also offer valuable experience for regulatory agencies across the world, and industry, to solve fintech-related challenges.

The Global Financial Innovation Network (GFIN) is a new model of international cooperation on fintech innovation and supervision that aims to increase collaboration between regulatory agencies in fintech and regtech. The network includes more than 60 financial services regulators, international organizations such as the IMF and World Bank, and other observers. Founded in 2018, it provides a venue for engagement and sharing of lessons learnt on fintech aspects and has three workstreams: (i) cooperation and sharing innovation experiences; (ii) forum for joint work and regulatory trials, including regtech; and (iii) providing an environment to test cross-border solutions. As part of the latter workstream, GFIN organized a cross-border solution pilot that attracted 44 applicants, of which eight were accepted. In the end, none of the selected firms could develop testing plans that satisfied the criteria of the participating supervisors. Moreover firms were not able to find regulated firms in other jurisdictions to joint-test with and, in some cases, the activities proposed were not part of the mandate of participating agencies. The new post-pilot cross-border test (ongoing) has incorporated lessons learned, including clarifying the mandates of participatory agencies in a regulatory compendium and centralizing the application process.[77]

---

73. CGAP 2020 blog: Digital Finance: Cybersecurity Requires Deeper Industry Collaboration.
74. The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors.
75. See also FSB Standing Committee on Supervisory and Regulatory Cooperation; FSB Innovation Network; and FSI publications and training.
76. See more details at https://www.r2accelerator.org/nigeriadatastack.
77. https://www.thegfin.com/compendium-1.

EMDE supervisors can also find key support with IFIs with near-universal memberships. The IMF organizes an annual Fintech Roundtable for supervisors with broad EMDE participation, conducts training and workshops on the challenges of fintech regulation and supervision in various jurisdictions, and has organized regional Bali Fintech Agenda Outreach Conferences. For example, the World Bank is working on strengthening the institutional capacity of financial sector regulators and other authorities (IMF and World Bank 2019). Examples include: capacity building and fostering dialogue through focused roundtables in Bangladesh, Colombia, Georgia, India, Peru, and Saudi Arabia; the modernization of core central bank and financial sector regulatory functions through extensive use of technology in Afghanistan, Burundi, and Vietnam; and supporting greater adoption of technology by commercial banks, microfinance institutions and credit unions in Afghanistan, Mozambique, and Sierra Leone.

5. Fintech Failures: How to Protect Customers' Funds and Financial Stability

Although hundreds of startups in the fintech domain fail every year, discussions around what happens when these failures take place are rather rare. Many jurisdictions have specific crisis management arrangements for financial institutions, aimed at preserving financial stability, the integrity of the financial sector, and savings of investors, corporates, and households. Yet, for the most part, these regimes are not readily applicable to fintech firms; and even if they were, most fintech firms do not need crisis management rules to be liquidated. Moreover, in most jurisdictions, the fintech sector is still in the early stages and putting in place specific wind-down mechanisms does not seem justified. Standard bankruptcy rules, coupled with strong consumer-fund protection measures, can work just fine until there is a clearer picture of the fintech landscape and more specific approaches can be devised.

For fintech firms that work solely as intermediaries of transactions, the financial risks are limited and no hard wind-down arrangements are needed. This is the case, for example, of peer-to-peer (P2P) lending providers, which connect borrowers to lenders and manage the underlying transactions, and robo-advisors, which work like investment brokers, connecting investors to the stock market, mutual funds, and other investment opportunities. In case a fintech firm engaged in P2P lending fails, the lenders will keep their credits against the borrowers, so their financial exposure will not change. However, to collect their debts, the creditors will need to access documentation and back-office services of the fintech firm. For this reason, authorities usually require P2P platforms to ensure that clients can promptly access their documents and transactions, including exit plans containing details of technologies used and steps necessary for the authority, a temporary administrator or a potential buyer of the failing firm, to access the data on transactions and make them accessible to clients.

Licensed institutions (whether incumbents or fintech startups) may be subject to a specific resolution regime. As is the case for regulation and supervision, fintech firms that engage in the same activities as traditional financial service providers should be treated, for crisis-management purposes, as traditional providers. Physical branches are not essential to the business model of, for instance, a bank or a broker-dealer, and moving their services online (for example, virtual banks or robo-advisors) does not change the underlying reasons why these businesses were regulated in the first place. In that sense, not only do virtual banks[78] need to be licensed and supervised as banks, but also the financial safety net, including provisions on resolution and deposit protection, should apply.

Non-bank fintech firms may become systemically important, in which case special wind-down arrangements are needed. Financial authorities must evaluate the potential impact of the failure of a systemically important fintech firm and address all major concerns appropriately. However, the lack of international standards or recommendations is a challenge, especially for EMDE countries with capacity constraints. In this note we offer some considerations that aim to help authorities tackle this challenge.

78. The term "virtual banks", as used here, refers to those institutions that undertake financial intermediation using non-traditional platforms. This does not include institutions that may be designated as "banks" but do not engage in traditional banking businesses, such as, for example, the "payment banks" existing in Mexico and India or the "foreign exchange banks" existing in Brazil.

5.1 Arrangements for Winding Down Fintech Firms

A well-designed wind-down regime should seek to minimize value destruction by mitigating the financial, economic, and social costs associated with the failure. The purpose of a resolution regime for financial institutions is: (i) to maintain financial stability and (ii) to ensure continuity of critical functions to the financial sector and the economy, such as payments, clearing, and settlement services. In devising potential mechanisms for winding down fintech firms whose failure could affect financial stability, some of the global principles for the resolution of financial firms (the *Key Attributes of Effective Resolution Regimes for Financial Institutions ("Key Attributes",* FSB 2014)[79] can serve as an inspiration, when relevant and applicable.

Departures from a regular insolvency regime are only warranted in those cases where there is a public interest to do so. For certain firms offering fintech services, regular insolvency regimes may not be feasible due to their potential systemic impact over the financial sector and the economy. This may happen due to the size and systemic importance of the firm (that is, when they are "too-big-to-fail." For example, large fintech firms engaged in payment transactions or large EMIs) or to the simultaneous failure of several players on the same market (that is, when there are "too-many-to-fail"). This assessment must be done at all relevant market levels (local, regional, and national). For example, in remote communities, often underserved by banks, closing the only financial institution that is present could have a significant impact on the local economy despite not being relevant at the country level. Moreover, as mentioned in the Basel Committee Guidance on Financial Inclusion (BCBS 2016), *"In some countries, non-bank financial institutions, while not systemic based on the value of funds they intermediate, may present a systemic dimension due to the number and type of customers they serve."*

The orderly wind down of a fintech firm should be conceived as one component of the broader financial institutional framework. Without proper regulation and supervision, prudential authorities will not have the necessary mechanisms to monitor the eventual deterioration in the situation of a fintech firm and attempt an orderly wind down. Consequently, countries adopting a "Wait and See" or "Test and Learn" approach to a fintech segment will hardly be able to depart from the standard corporate insolvency regime in case of failure. Moreover, it is good practice to have proper separation between the authorities in charge of supervising and those in charge of winding down fintech firms. Yet, for jurisdictions in which fintech firms are regulated and supervised by the bank supervisor, the resolution of fintech firms could be assigned to the bank resolution authority, with due arrangements that ensure the independence of both functions.[80] The wind-down authority or division should have a strong knowledge of the underlying technologies and the interconnections of fintech firms to be able to assess the impact of a failure and develop adequate strategies to address it.

Tools and powers for winding down fintech firms must be established in the law. The application of tools to wind down a firm goes beyond the supervisor-supervised relationship and affects the rights of third parties independently of their consent (for example, when allocating losses to shareholders and creditors). Therefore, these tools need to be established in the law (rather than in second order regulations) to ensure that (i) all stakeholders are aware of their rights, obligations, and risks in case of a failure and (ii) the proper safeguards are in place. Tools that are usually applied in bank resolution and which could be used to wind down fintech firms include the following:

- **Determine adjustments in firms' practices to ensure the feasibility of winding-down mechanisms,** including practices related to the storage of client data and access to proprietary technology.

79. Among others, the Key (resolution) Attributes make reference to the need for:
    - Ensuring the continuity of systemically important financial services, and payment, clearing, and settlement functions
    - Protecting, where applicable, depositors, insurance policyholders, and investors as are covered by such schemes and arrangements, and ensure the rapid return of segregated client assets
    - Avoid relying on public support and not create an expectation that such support will be available.
80. As a reference, the Key Attributes require that jurisdictions have a designated and independent administrative authority responsible for bank resolution. If this authority lies with the same agency responsible for supervision, separate reporting lines are necessary to ensure independence.

- **Establish a provisional administration regime** to take over the firm, replace existing management and attempt to transfer the business to potential acquirers and, where such a transfer is not possible, to phase it out in an orderly fashion.
- **Transfer assets and contracts to third parties,** including those contracts related to intellectual property and software licenses, without requiring the consent of the firm or its customers.

5.2 E-Money Institutions: The Importance of Protecting Customers' Funds

The best way to ensure the availability of funds when an Electronic Money Institutions (EMI) fails is to ringfence client reserves by law, although this is still not prevalent in a number of jurisdictions. As explained in section 3.3.1, prudential regulations stipulate that non-bank EMIs, regardless of their size, must preserve the funds entrusted to them by their clients. The best way to support this prudential goal is to make these funds "bankruptcy remote" by law so that the creditors and courts cannot use them to settle the failed EMI's liabilities. Statutory ringfencing is recommended regardless of the size of the EMI to avoid any monetary loss to customers. For systemic EMIs, the ringfencing should be established along with the specific wind-down mechanisms discussed in section 5.1.

Authorities must put in place mechanisms to ensure the access to the ringfenced funds upon failure of an EMI. In principle, failures could be dealt with by transferring the ringfenced funds and accounts to another issuer with minimum disruption. However, fintech firms usually operate with proprietary technologies that cannot be easily transferred to another player's system and this may hinder the process. Authorities need to be well versed in the underlying technologies and aware of any interoperability options. They could also request EMIs to prepare "exit plans", where they explain how their technologies can be transferred in case of need and set regulations requiring a minimum degree of interoperability to increase the likelihood of timely and successful transfers of funds.

Ringfencing does not eliminate the risk of fraud, misappropriation of funds, or operational risks such as from technology shortcomings or issues related to agent networks. Some form of deposit insurance, as discussed below, may be required to address these kinds of situations. In any case, adequate regulation and supervision remain key elements to mitigate these risks, ensure confidence, and avoid undue stress on the payments system and the real economy.

Most countries have implemented some form of fund segregation to facilitate access to customers' funds in case of failure. EMIs are usually required to keep client funds separate from other assets, including their own funds. This "segregation" practice is not equivalent to or a substitute for ringfencing, but rather a complementary measure that facilitates access to the funds when needed. Some countries (for example, Brazil, see box 7, or China) require that they are either deposited with the central bank or invested in government bonds, which is the safest approach. A more common approach, however, is to require fintech firms to deposit clients' funds in special accounts with one or more commercial banks.

Box 7. Treatment of E- Money Institutions (EMI) in Brazil

The Central Bank of Brazil's Circular 3681 of 2013 establishes (art. 12) that issuers of e-money must keep liquid resources corresponding to (i) all the balances kept in customers' accounts, plus (ii) amounts in transit between accounts of the same issuer, plus (iii) amounts received by the issuer but not yet credited to its customers' accounts. At the end of each business day, these amounts must be either deposited in kind in a special account at the central bank or invested in treasury bills under the central bank's custody.

According to the authorities, the rationale for this requirement is that EMIs are not financial intermediaries and should not use customers' funds for any purpose. Their business model is fee-based, and the funds deposited by customers

should not be incorporated into their assets. Due to Circular 3681, coupled with legal provisions that make EMI reserves bankruptcy-remote, if an EMI fails, customers' funds are not affected and may be promptly returned to them.

To allow EMIs to offer more attractive products and better compete with traditional banks, Circular 3681 allows them to pass on, to the e-money holders, the remuneration received on the investments in treasury bills, in whole or in part.

The requirement to keep the reserves deposited at the central bank or invested in treasury bills was introduced in phases (20 percent of balances from May 2014, 40 percent from January 2016, 60 percent from January 2017, 80 percent from January 2018, and 100 percent from January 2019), to allow issuers to adapt.

The resilience of this structure was showcased in 2018 during the failure of Banco Neon, a licensed bank which had a joint venture with Neon Pagamentos S.A., an EMI. Despite the same name, both institutions had separate ownership and were not part of the same financial conglomerate. Pursuant to the joint-venture agreement, Banco Neon was responsible for the settlement of transactions entered into by Neon Pagamentos on behalf of its clients. When Banco Neon was liquidated, all customers kept full access to their funds because client reserves had been stored at the central bank in accordance with Circular 3681.

Allowing EMIs to deposit funds in commercial banks is not as safe as requiring that reserves are kept with the central bank or invested in government bonds, because commercial banks can fail. Some countries are dealing with that extra layer of risk by extending the deposit insurance protection directly to EMI customers, as if they were the holders of the amounts deposited in the failed bank. This, however, presents additional challenges, as explained in the next subsection.

When funds are safely ringfenced clients should be informed to promote confidence and stability. Although EMI runs will not cause the same liquidity shock as bank runs, they can be extremely stressful for the fintech firm. Moreover, where issuers have a significant role in a country's financial system (for example in Africa, see box 4), their failure can have a strong negative impact over the payment system and the economy as a whole. However, in countries where EMIs are allowed to deposit client funds in commercial banks, ringfencing may be of little use if the bank fails and the funds are lost.

5.3 Electronic Money and Deposit Insurance

As EMIs expand their market share in the "deposit-taking" landscape, the question arises as to whether they should also be covered by the deposit guarantee scheme. At first thought, Deposit Guarantee Schemes (DGS) are an obvious way to protect customers. However, even though e-money accounts may be seen by the client as similar to deposits (in some jurisdictions part of the success of EMIs is the ability to mimic bank accounts from the client's perspective), they are very different in terms of risks. There is a substantial difference in deposits collected by institutions allowed to intermediate funds (for example, banks and credit unions) and those collected by institutions not allowed to do it. In the first case depositor is a creditor of the institution while for EMIs, funds are held solely in custody on behalf of the client.

If proper ringfencing measures are in place, a deposit insurance fund would be redundant. If the clients' funds are effectively ringfenced (that is, protected against the fintech firm's creditor claims), they are already available to reimburse depositors promptly. Consequently, there would be no need to have a second pool of resources (the deposit protection fund) to that same end. However, few jurisdictions have statutory ringfencing arrangements in place, and even when this is the case, it is common to allow EMIs to deposit their reserves in commercial banks, with the risk of losses if the commercial bank fails.

In some countries where a statutory ringfencing is not feasible, the "direct approach" applies, whereby EMIs are direct members of the Deposit Guarantee Scheme (Izaguirre et al., 2019, 2015). There are two main advantages of this approach: the first one is that it addresses those scenarios where the EMIs' reserves are not sufficient to pay all e-money holders, due, for example, to fraud or misappropriation of the funds by the EMI. The second advantage is that, by becoming a member of the deposit insurer, the e-money provider will have to comply with regular reporting obligations to the deposit insurer, facilitating payout to customers in case the provider fails. However, while protecting consumers of e-money is an important policy measure, especially in jurisdictions where e-money is responsible for a significant market share, including EMIs as members of the DGS might not always be optimal, as explained below.

A decision to protect the holders of e-money would have to be based mostly on consumer protection considerations, rather than on the fear of contagious runs by healthy market players. The main purpose of a DGS is to protect financial stability by reducing the likelihood of bank runs, a risk that EMIs do not have. Bank runs may cause the failure of otherwise perfectly healthy institutions since a high percentage of depositors demand their money back at the same time, eating up all of the bank's liquid assets and pushing it towards insolvency. By ensuring compensation for any deposits unpaid (up to the stated coverage rates) and assuring depositors of other banks that their funds are safe, the DGS removes the incentive for depositors to withdraw their funds on news of failure, limiting the crisis to the failed bank and mitigating the contagion effects. Ultimately, by contributing to a system where depositors of a failed bank are protected, all members of the deposit insurance benefit from the lower risk of contagion. In contrast, EMIs are not exposed to the risk of "contagious runs" because they do not (and should not) engage in maturity transformation. As explained in section 5.2, EMIs must safekeep their customers' funds. This means that even if a run happens on a healthy EMI and all customers decide to withdraw their money at once, the EMI should be able to return the funds, despite loss in profitability and further negative impact over its business.[81] In such circumstances, one needs to consider whether contributions funds paid by the industry to the DGS (in the form of premiums or contributions) would be the best mechanism to finance consumer protection, or whether such a policy would be better financed with other sources of funding.[82]

As the e-money business relies on very thin margins, the inclusion of EMIs in a DGS scheme, with the obligation to pay premiums, may impose an excessive burden on their business models. As banks can intermediate funds at a spread, they can direct part of that spread to fund the DGS premiums. EMIs, on the other hand, are just safe keepers of client reserves and do not make profits on them. Their business model is usually based on charging a small fee for every transaction with the e-money issued by them. Requiring them to pay premiums to a DGS may force them to charge significantly higher fees both from customers and from merchants. More importantly, this increased cost would only bring marginal benefits, covering only the risk of fraud or misappropriation of the funds, given that, as explained above, in the absence of such situations an EMI will not face significant liquidity mismatches.

When EMIs are required to deposit client funds in commercial banks it might make sense to extend the DGS coverage to such reserves to protect them against the eventual failure of the bank. As mentioned above, in jurisdictions where EMI can deposit funds in commercial banks—be it through escrow accounts, trust accounts or other arrangements—reserves will be at risk if the commercial bank fails. This, in principle, would leave the technological platform intact, but the customers' funds would be inaccessible or lost. Izaguirre et al., 2019, report that, to address this risk, some countries have extended DGS coverage to EMIs using the "indirect" or "pass-through" approach. In this approach, if a commercial bank, which is the depository of e-money reserves, fails, the DGS will treat each of the e-money holders as if they were depositors in the bank, insuring each of them up to the maximum amount applicable to the bank's depositors. In other words, the deposit insurer will look-through, or pass-through the EMI and cover its customers directly. In this case, premiums over the deposits would be paid by the commercial bank (thus limiting the impact over the EMI's business model).

---

81. The picture would be of course different if the EMI is failing and there are no ringfencing provisions in place. In this case, e-money account holders will compete with other creditors and may not be able to get fully reimbursed.
82. The failure of a large EMI may disrupt payment systems and have negative impacts on the real economy. Yet, the solution to this is not necessarily a large pool of DGS resources, but rather a swift re-establishment of the access to the payment platforms.

The pass-through approach can be an efficient mechanism to protect customers' funds in some cases, but it poses challenges to the deposit insurer and it is yet to be tested. Adequate measures should be in place to mitigate moral hazard and the DGS needs to have good access to information on client identification and balances. For example, identifying customers of the EMI can be complex, given the high volatility of balances in these accounts. Reconciliation of balances is also a significant challenge and might render the deposit insurer unable to reimburse e-money holders quickly, undermining the reputation of the DGS. This can be mitigated by allowing alternative forms of compensation, such as giving the deposit insurer powers to transfer the (full) reserves to a sound bank so that the EMI can continue its operations or paying the insured amount directly to the EMI, which then will be in charge of making the money available to its customers. The determination of DGS premiums based on risk indicators (that is, the DGS exposure to the EMI failure) may also be challenging, given that EMIs do not usually report to the deposit insurer. The challenges of the passthrough approach can be exacerbated substantially if the EMI fails alongside with the bank where the funds are deposited. In this scenario, the technological platform of the e-money provider may not be available for the deposit insurer to deliver payment to the holders of e-money, which could substantially delay the payout.

In the absence of adequate safeguards, the pass-through approach may also result in moral hazard. When an EMI is not at risk of losing a significant portion of the reserves if the bank fails (because the DGS will cover the amounts under the pass-through approach), it may be tempted to place such reserves in a sub-optimal manner (for example, deposit in an unsound commercial bank in exchange for higher interest rates). A country adopting the pass-through approach must ensure that there are proper mechanisms in place to address this risk of moral hazard, such as requiring EMIs to have adequate risk-management functions and ensuring that their choice of depositor bank is made for the right reasons.

Regardless of which option is adopted, public awareness remains a crucial aspect of deposit insurance. Clients must be made aware, and constantly reminded, of the risks involved in the products they use, the mitigation measures in place, and the limits of such mitigation aspects. In that sense, a country using solely the pass-through approach for deposit insurance must ensure that customers know that losses due to misconduct of the e-money provider would not be covered since there will not be enough segregated funds to cover them.

6. Concluding Remarks and Recommendations

Reaping the benefits from fintech will require adapting and strengthening regulatory and supervisory frameworks, including through increased cross-agency and cross-country collaboration. The high dynamism of the fintech market, and the accelerated speed at which it is opening the door to new players and business models, suggests that this may be a challenging endeavor, especially for EMDEs with capacity constraints and multiple competing mandates (FSI 2021). But the cost of inaction can be high, with network effects pushing towards rapid changes in the landscape and costly ex-post adjustment efforts (Boot et al., 2020). As fintech penetration increases so will associated potential risks for consumers and investors, stability, and integrity. While there is no silver bullet to strike the right balance between keeping these risks at bay (which should be the priority) and promoting development through innovation and competition, the closest the policy response gets to ensuring certainty and consistency, proportionality, and technology neutrality, the higher the probability that the balance will be right.

The main conclusion of this note is that financial authorities will need to manage financial risks associated with fintech through a timely and proportionate policy and supervisory approach that preserves the stability, safety, and integrity of the system while avoiding, as pertinent and feasible, imposition of unnecessary barriers to development, innovation, and competition. The below recommendations, which are not meant to be exhaustive, develop further these ideas.

Recommendation 1. Assess the fintech landscape, risks, and regulatory gaps at an early stage

An assessment of the fintech landscape, potential development benefits, and implied risks for financial stability, integrity, and safety is key to identify regulatory gaps and inform a timely and sound policy response. Existing and potential risks will be determined by the fintech activities and firms that operate in the market, their degree of maturity, penetration, and interconnectedness across the financial system. Authorities should look carefully at the most relevant (larger and/or more interconnected) fintech players operating in their jurisdiction with a forward-looking approach to understand how they operate (as standalones or as partners with banks) whether they should fall under their remit or not, be it through full supervision under a license or mostly through monitoring and oversight. This is especially relevant when a fintech company is a subsidiary of a non-financial group, since they will not already fall in the regulatory perimeter. Supervisors need to be vigilant in their markets by continued monitoring of the fintech marketplace through an innovation office, a targeted engagement, or the use of suptech tools.

Recommendation 2. Set clear policy goals with core surveillance and oversight mandates as a priority

Before undertaking any regulatory action, the adequacy of the existing framework must be assessed, including its legal foundations. All foundational sectoral laws (for example, on consumer protection, cybersecurity, competition) as well as foundational legal concepts (enforcement of contracts, e-signature, data ownership, insolvency, etc.) must be in place to ensure the success of any regulatory action in the fintech domain. The priority for financial regulators must be to ensure the core surveillance and oversight objectives of (i) preserving financial stability, (ii) ensuring integrity; and (iii) protecting consumers and investors. When applicable, the assessment could also consider whether and how the existing framework would allow for the achievement of specific fintech policy objectives determined by the national authorities (inclusion, competition, innovation, etc.).[83]

83. This assessment could be undertaken by an inter-agency working group appointed by the regulators or alternatively, by external advisors.

Authorities must provide legal certainty through a clear definition of the regulatory perimeter and associated requirements. Innovation is oftentimes hampered by unclear or cumbersome regulation. It should be clear when and how regulation applies and what are the obligations and requirements to be met by each player (even in cases when regulation is activities-based, it is always the provider, as a legal entity, who ultimately must meet the regulations). Regulators should be unbiased towards the use of a given technology provided that the service provided is safe and reliable both at the client and system level.

Authorities should consider going for a new bespoke framework only when simpler options are not feasible. When a fintech activity is not already included in the regulatory perimeter, the authorities have three main options. First, they can allow the activity without including it in the regulatory perimeter (issuing a permissive instrument such as a letter of non-objection; deliberately deciding to take a passive/hands-off stance; allowing a pilot in the context of an innovation facilitator). This light-touch approach would only be safe when the activity presents very low risks, including in terms of regulatory arbitrage and level playing field alteration. Second, regulators can bring the activity (or its provider) into the perimeter if the existing regulation allows so with some amendments. Finally, the regulatory analysis and consultation processes may point to the need for a new bespoke framework to include or prohibit the fintech activity. Setting up a new framework can be a cumbersome approach, as each new business model, new technology, or new provider entering the product space could require further new regulation. Therefore, regulators should be cautious when embarking on bespoke solutions, especially if they are being used as a stopgap solution rather than as the result of a well-conceived regulatory strategy.

Recommendation 3. Set proportionate and tech-neutral prudential and conduct requirements

The regulation should be focused on the systemic relevance of the provider and the function of the activity or service provided, rather than the type of institution offering it, per se. It should target the activities, in particular the functionality provided, without any specific technology in mind. This ensures a level playing field for all service providers and avoids inefficiencies associated with regulations needing to be constantly updated or reviewed due to changes in the nature of the providers. However, in some cases, the nature of the core business of the fintech provider and potential interconnections with the rest of the financial system imply that an entities-based approach might be warranted. This is the case with (potentially) systemic fintech firms such as big tech firms, for example.

Regulatory requirements should be proportionate to the risk profile of the fintech activity and systemic relevance of the providing entity (when applicable). A disproportionately strong regulatory response could place excessive regulatory burdens over new entrants and activities, hindering innovation and competition to the detriment of financial efficiency, inclusion, and overall development goals. Yet, a too lenient policy response could lead to the build-up of unmonitored risks, including potential cybersecurity and financial integrity breaches, consumer abuse practices, and an uneven playing field where new entrants engage in regulatory arbitrage to the detriment of incumbents, which could ultimately jeopardize financial stability. To balance this out, regulators should avoid placing constraints over the development of those small or non-complex fintech activities that do not pose material (potential) risks.[84] For example, while bank-like prudential requirements might make sense for fintech activities that engage in maturity transformation or that hold customers deposits in their balance sheet, this will not be the case for firms that simply provide a means for payment or a software, unless the supervisor considers that new or exacerbated risks (for example operational) could be introduced or amplified by the fintech activity. In that regard, a risk-based supervision approach to fintech is warranted, as it provides authorities with a prioritized guide regarding the entities and activities with the highest regulatory risk.

84. Restoy, F. "Proportionality in financial regulation: where do we go from here?" BIS, FSI speech. May 8, 2019.

In the absence of a competition mandate, financial sector regulators have several regulatory levers they may want to use to promote competition while safeguarding their core stability and integrity mandates. Financial sector regulators should understand the synergies and relationship between financial regulation and competition and choose the best option that supports competition while fulfilling their core mandates, possibly using the following levers:[85]

i. When drawing the regulatory perimeter and establishing licensing frameworks, look at fair market-entry aspects, including licensing and capital requirements.
ii. Through regulation, consider promoting a level playing field for all stakeholders on issues such as distribution (agency banking and mobile-money agents), data (open banking regimes), customer due diligence (eKYC and tiered customer due diligence).
iii. In combination with their consumer protection mandate, when this is the case, they can require price transparency and disclosure to allow customers to compare terms and prices. Financial sector regulators must ensure that provisions exist concerning disclosure of terms and conditions, transparency of pricing, safety of any funds, agent liability (if applicable) and effective dispute and recourse mechanisms.
iv. Collaborate at the domestic level with industry regulators (for example, for telecoms and other utilities that may offer financial services) as well as competition and data protection authorities. Also at the international level to coordinate policies and help to ensure regulatory consistency and peer learning between countries.[86]

Recommendation 4. Define a clear strategy to promote operational resilience

Supervisors must be aware that operational risks will be amplified. IT disruptions, regulatory risk, cyber breaches and data compromises, fraud, and outsourcing risks are likely to increase in a financial sector with an increased fintech footprint. The potential for operational disruptions requires supervisors to revisit, adjust, or expand their own approach to risks arising from fintech to ensure that fintech providers and financial firms relying on their services have appropriate corporate governance and risk-management structures in place. The supervisory strategy to foster operational resilience in the industry should include issuance of clear Operational Risk-Management rules and guidance that require an active involvement by senior management of the firm. Competent oversight agencies should expect banks and fintech under their purview to have expertise, financial acumen, and a risk-management framework commensurate to their risk profile.

Supervisors should have a clear vision of what is needed to mitigate cyber risks and communicate their strategy accordingly. To that end, a useful reference tool for supervisors is the G7 Fundamental Elements of Cybersecurity for the Financial Sector that covers key aspects of cyber-risk governance, risk identification, and resilience.[87] The regulatory digest published by the World Bank Group is another valuable resource for any jurisdiction seeking to build up its supervisory processes based on best international practices.[88] Market intelligence should also inform any supervisory approach, especially for cybercrime. According to external analysis, fintech companies that experienced ransomware attacks already exhibited weaknesses in their IT systems. Supervisors should be attentive to any relevant insights coming from reliable external sources signaling problems that could prompt further analysis and timely supervisor responses.

Recommendation 5: Scale up capacities and resources according to the specific challenges posed by fintech, including when using regtech and suptech solutions

Fintech-related changes may require financial supervisors to reassess their current supervisory models and resources to continue to ensure effectiveness of their oversight function. To keep up with market developments

85. In implementing these regulatory levers, regulators can use certain regulatory tools to ensure that the competition objective is duly considered once the primary objectives of stability, safety, and soundness are ensured. These tools include Regulatory Impact Analysis frameworks (to determine the change affected by regulations and policies and isolate the right variables to achieve the regulator's objectives) and the OECD competition assessment toolkit (to identify unnecessary restraints on market activities and develop alternative, less restrictive measures that still achieve government policy objectives).
86. See Plaitakis and Soursourian, 2019; Feyen et al., 2021.
87. The eight elements represent the high-level objectives and supervisory expectations of any financial institution in charge of managing cyber-risk exposure.
88. The publication produced under the auspices of the Financial Sector Advisory Center and titled *"Financial Sector's Cybersecurity: A Regulatory Digest"* offers a comprehensive compilation of recent laws, regulations, guidelines, and other significant documents on cybersecurity for the financial sector.

and innovations, authorities need to ensure that the knowledge, skills, and tools of staff remain relevant and effective to supervise innovative business models. Producing a map of the skills gap is highly advisable. To that end, the agency needs to identify the different types of expertise required to supervise fintech developments. This includes disciplines like data science, business intelligence, and other emerging skill sets like artificial intelligence, machine learning, and blockchain. Once this inventory has been completed, the supervisory agency should find out where it currently stands in terms of staff qualification by comparing the skills required from staff against the skills they possess.

Building proper IT expertise is also warranted. The authorities should have capable IT experts who can support in understanding the heavily tech-dependent business of fintech companies. In many EMDEs, it will not be easy to build this capacity in-house, without hands-on exposure. Having room to hire experts from the private sector or introduce secondment programs among supervisors would be important.

Closing the supervisory skills gap needs to be well thought out and planned. This is one of the most challenging undertakings for supervisors in the context of fintech. It can consist of a combination of in-house training for existing staff and recruitment of newly-qualified people. Supervisory agencies will compete with many other players looking to attract highly qualified experts.[89] Also, upskilling existing staff can be more efficient and cost-effective than recruiting and onboarding new candidates, but in order to succeed, training programs need to be constant and consistent to ensure that current skills will stay relevant.

Suptech and regtech solutions can be an excellent resource to overcome supervisory constraints. The technological changes that have enabled fintech to thrive can be leveraged to improve supervisory processes. This is the promise of suptech, defined as the use of innovative technology by financial authorities to support their work.[90] Machine-readable and executable regulation, automated Artificial Intelligence solutions for data input, aggregation and analysis, and platforms linked to regulation offer a wide range of opportunities. Suptech has the potential to bring efficiencies, both for supervisors and supervised entities, in processes such as data collection, quality control, monitoring and detecting suspicious activities,[91] reporting and disclosure, analytics, and risk management. Many financial authorities have a suptech strategy, often as part of an institution-wide digital transformation program, and others have adopted ad-hoc suptech projects. However, the use of suptech requires having staff with appropriate skills, which might be difficult for some emerging countries. In some cases, countries have resorted to contracting external vendors to develop suptech solutions, but this presents risks if the work is not properly understood and monitored by the supervisor, leading to "black box" and reputational risk.

Recommendation 6. Cooperate both domestically and internationally

Considering the cross-sectoral nature of many fintech businesses, including that of big tech firms, cooperation among domestic agencies is key. Different sector regulators might be involved in the regulation and supervision of a given fintech activity or entity, including, but not limited to, the national treasury, the prudential authorities, the central bank, the financial sector conduct authority, national credit regulators, securities exchange authorities, financial intelligence units, competition authorities, telecom authorities, and authorities in charge of data protection. Authorities can sign memoranda of understanding (MoUs) to facilitate fruitful cooperation among all competent authorities and key stakeholders on issues of common interest such as the regular exchange of information or strategic cooperation in the prevention and management of crises. These MoUs will establish terms of the cooperation, on the basis of mutual trust and understanding, with full respect to the respective mandates and competencies.

---

89. Even in countries known for a workforce highly proficient in information technology and computer programming such as India, the labor pool for digital financial services is drying up. See "Mondato, Solving the Skills Gap in Digital Financial Services." October, 2018.
90. See "The Suptech Generations." FSI insights no. 19 (2019).
91. A greater use of transaction accounts comes with more opportunities for customer abuse—in part owing to still low degrees of financial literacy—and fraud, but it also generates large quantities of machine-readable data, for which tools such as network analysis of suspicious transactions can be useful. See FSI Insights 9 (Innovative Technology in Financial Supervision (Suptech) —The Experience of Early Users), FSI Insight 18 (Suptech Applications for Anti-Money Laundering) and FSI Insight 19 (*ibid*). See also Toronto Centre, 2017 and 2018.

Collaboration between regulators/supervisors and fintech providers is recommended as it opens up opportunities for both. A regular dialogue with fintech developers, providers, and incumbents greatly facilitates capacity building within the competent authorities and raises the private sector's awareness to the risks and their regulatory obligations, especially with respect to AML/CFT, consumer protection, and transparency. Supervisors are therefore encouraged to engage with the industry, including via private/public working groups, conferences, and workshops.

International supervisory cooperation is also essential. Given the cross-border dimension of fintech, especially for products such as mobile money and digital remittances, supervisory actions in one jurisdiction are unlikely to be fully effective without coordinated action elsewhere. As a result, strong international supervisory cooperation will facilitate knowledge transfer and sharing of international best practices. International cooperation could be particularly helpful for agreeing on standards to develop regtech and suptech solutions that are compatible across countries. There are multiple examples of bilateral international collaboration agreements between financial agencies. Engaging with international bodies and networks such as the FSB, BIS fintech hub, or GFIN can also bring a lot of benefits, for example, in sharing experiences and ideas and getting insights on latest developments. IFIs such as the WB and the IMF can also provide technical assistance and advice to emerging countries.

Recommendation 7. Establish safe mechanisms to protect customers' funds in case of failure of electronic money institutions and also to wind down systemic fintech firms.

Special wind-down procedures are only indicated in cases where the fintech provider has a systemic relevance. The rest of fintech failures can be dealt with through regular bankruptcy procedures. In the absence of targeted international standards for resolution of fintech firms, it is recommended that wind-down frameworks provide authorities with powers and tools to be able to, among others, (i) appoint a provisional administrator and (ii) transfer contracts without consent of the firm or its customers. Authorities could also consider instituting powers to mandate adjustments to fintech firms' business models to facilitate their winding down. The framework should also include requirements for the systemic firms to prepare "exit plans" to allow for their swift winding down, supporting the continuity of services and access to funds. Such plans could list the steps necessary to transfer the firm's platforms and include details on proprietary technologies or software licenses.

Authorities are encouraged to require that e-money institutions adequately ringfence their clients' funds and keep them segregated from the institution's own assets in a safe place. This will ensure that they are readily available and easily transferable in case of failure, especially if they are kept in government securities or deposited with the central bank. Where this is not possible, and reserves are to be placed with a commercial bank, consideration could be given to extending the coverage of the deposit guarantee scheme (DGS) to the balances of e-money accounts deposited by the EMI with the commercial bank. However, this "pass-through" approach presents technical challenges that would need to be addressed to ensure that payouts can be done in a timely manner.

Asking the EMIs to affiliate with the DGS directly would help protect customer funds, especially in case of fraud or misappropriation of e-money reserves. It has also the benefit of ensuring that the DGS has sufficient information to pay out customers if the fintech firm fails. However, this approach seems to go against the raison d'être of deposit insurers, as, in contrast to banks, EMIs are not under the risk of contagious runs and therefore have no obvious reason to mutualize the costs of failure of a competitor. An open question remains as to whether this type of consumer protection policy should be funded by the industry's (private) funds or by other (public) funding mechanisms.

Appendix 1: A Non-Exhaustive Review of Approaches Taken by Several EMDEs to Regulate Fintech

Selected Fintech Regulatory Strategies in Africa

The recent introduction of innovation facilitators—mainly regulatory sandboxes—allows African regulators to monitor and better understand a diverse set of fintech activities. Thirty-two percent of Sub-Saharan regulators surveyed by the World Bank and Cambridge Centre for Alternative Finance (2019) had a regulatory sandbox in place or in development. Interestingly, security regulators, in particular, seem to have an affinity for regulatory sandboxes, making up almost half of the sandboxes that are currently live or in development in Africa.

- **Sierra Leone's regulatory sandbox, established in 2018, has a financial inclusion objective and is expressly linked to Sierra Leone's *National Strategy for Financial Inclusion* 2017 – 2020.**[i] The initial cohort included a mobile platform to train low-income entrepreneurs which provides access to digital loans, a digital savings tool for farmers to assist input purchases, an interoperable e-money platform and an open payments API that allows third-party developers to connect to banks and mobile money networks.[92]

- **Mauritius launched a "Regulatory Sandbox License" (RSL) in 2018.**[93] Although the RSLs are issued to all eligible companies willing to invest in innovative projects and are not limited to fintech activities, there are special guidelines for fintech projects[94] and the majority of the first fintech Sandbox Licensees are focused on cryptocurrencies. These include a crypto-custodian service, a wealth management platform, which combines robo-advisory fund management, blockchain-backed custodian and conventional funds, a lending platform for blockchain-backed loans, a blockchain-based, decentralized identity management system, and an online equity crowdfunding platform.[95]

- **Kenya's Capital Markets Authority launched in March 2019 a Regulatory Sandbox for fintech firms that offer innovative products, solutions, or services with the potential to deepen Kenya's capital markets.**[96] In July 2019, three firms were admitted, including a cloud-based data analytics platform designed for use by investors, fund managers, custodian banks, actuaries, pension administrators, and regulators, and an internet-based crowd-funding platform through which investors can provide loan facilities structured as loan notes (debentures) for Small and Medium Enterprises (SMEs).[97]

---

92. Sierra Leone fintech Challenge—Press release.
93. See the Economic Development Board website here.
94. Regulatory Sandbox License—Guidelines for Fintech Projects.
95. The Economic Development Board: EDB issues Regulatory Sandbox Licenses to fintech companies for their innovative projects.
96. Capital Markets Authority, "CMA Regulatory Sandbox Ready to Receive Applications."
97. Capital Markets Authority, "Three Firms Admitted to the CMA Regulatory Sandbox."

- **Other African regulators with either live or in development regulatory sandboxes** include Central Bank of **Mozambique** (live since May 2018),[98] the Securities and Exchange Commission in **Nigeria** (in development), the **Rwanda** Utilities Regulatory Authority (in development),[99] the National Bank of Rwanda (live),[100] the Central Bank of Eswatini (live), the Central Bank of **Egypt** (live), and the Capital Markets Authorities of **Tanzania** and **Uganda**, under the umbrella of East African Securities Regulatory Authorities (EASRA) (in development)[101].

- **Regtech accelerators are also gaining ground,** including in Kenya (Capital Markets Authority) and Nigeria (joint initiative between Central Bank of Nigeria and Nigeria Inter-Bank Settlement System).

It is clear, however, that these innovation facilitators are only the beginning. A large majority of regulators in Sub-Saharan Africa are not actively regulating alternative finance activities for example. A survey by the WB and the Cambridge Center for Alternative Finance (2019) found only 12 percent of African regulators surveyed regulated equity crowdfunding, the alternative finance activity most likely to be regulated elsewhere.

Selected Regulatory Strategies in Asia

Asian regulators have taken a variety of approaches to fintech activities, depending on the type of service. Overall, we observe a more cautious approach to "first generation" fintech activities such as mobile payments and e-money, and a more active, hands-on approach to newer fintech business models such as digital lending and equity crowdfunding.

Asia has also seen the entrance of big tech firms into financial services in countries such as Bangladesh (bKash), China (Alibaba, Tencent, and Baidu) and Indonesia (GO-JEK), which has brought a new set of challenges to regulators (IMF, 2019). Big tech credit provision, in particular, has shown rapid growth in Asia, in countries such as China and Indonesia.[102]

The first attempts of Asian regulators to regulate mobile money and extend agent banking mirror, to a certain extent, the approaches African regulators have taken. As mentioned above, China's approach to mobile payments can be best characterized as "Wait and See". The Philippines took a similar approach to mobile money, allowing MNOs Globe and PLDT (through its subsidiary Smart) to pilot new mobile money products to their customers in 2004. These pilots were closely supervised by the Bangko Sentral ng Pilipinas (BSP), the central bank, but there were no new rules introduced at the time. The BSP undertook regulatory action only five years later, with the issuance of "Guidelines on Use of Electronic Money."[103]

Regarding agent banking, an important element in ensuring the distribution of mobile money, Indonesia's approach can be best described as "Test and Learn". Indonesia launched a voluntary Pilot Branchless Banking Program in 2013, allowing certain banks and/or MNOs (with central bank oversight) in a limited pilot to offer banking and payments system services through agents.[104] The pilots were implemented in close partnership with the central bank to extract learnings and experience. These shaped the subsequent new Branchless Banking (Laku Pandaia) regulations that were issued in November 2014, which expanded the number of financial institutions able to use agents.[105]

98. The Central Bank of Mozambique and the Financial Sector Deepening Moçambique (FSDMOÇ) launched the regulatory sandbox to promote innovation with "fintechs."
99. Rwanda Utilities Regulatory Authority, Draft Regulatory Sandbox Framework.
100. The New Times, "Central Bank Grants Testing Approval to Emerging Fintech Firm."
101. CMA Uganda, "East African Securities Regulators Agree on Criteria for Fit and Proper Assessment of Market Practitioners."
102. Financial Stability Board, "BigTech Firms in EMDEs: Market Developments and Potential Financial Stability Implications.", (to be published)
103. John Schellhase and Amos Garcia, Milken Institute, "Fintech in the Philippines: Assessing the State of Play."
104. Ivo Jenik and Kate Lauer, CGAP Working Paper, "Regulatory Sandboxes and Financial Inclusion."
105. Ibid.

Other Asian regulators have taken a more conservative and phased approach to regulating e-money, leveraging on African and Philippine experiences. They first focused on extending mobile money to banks and only included non-banks in the regulatory perimeter once the international experience in countries such as Philippines and Kenya paved the way. Sri Lanka initially required MNOs to enter partnerships with regulated financial institutions. In August 2007, the Central Bank of Sri Lanka (CBSL) authorized the National Development Bank (NDB), a licensed commercial bank, to launch a mobile banking service called eZ Pay in partnership with MNO Dialog. After closely monitoring the market, analyzing the experiences of peer countries, and observing the lack of mobile money adoption, the CBSL issued in 2011 two sets of mobile payment guidelines—one for banks and one for non-banks—that allowed both banks and non-banks to offer mobile payment.[106] Similarly, Bangladesh issued its Mobile Financial Services Guidelines in 2011, allowing only scheduled commercial banks and their subsidiaries to provide mobile financial services. It was only with the issuance of the Mobile Financial Services Regulations in 2018 that non-banks were allowed to become a special type of e-money providers that could offer payments from an e-money account.

Regarding "second generation" fintech activities, such as digital lending and equity crowdfunding, the Asian regulatory approach has become generally proactive, with the issuance of specific activity-focused regulations at an early stage of market development. This may be in part a reaction to China's initial experience with peer-to-peer (P2P) lending platforms, whose aggressive growth can be attributed to a lack of regulation for almost a decade, but which also led to multiple scams and controversies, finally pushing the Chinese regulators to intervene in 2015.[107]

Thailand issued the first regulations for equity crowdfunding (ECF) in the ASEAN region on May 15, 2015. These have since been replaced by new regulations issued by Thailand's Securities and Exchange Commission on May 16, 2019 that magnify the scope of permitted crowdfunding activities. The new regulations now allow issuers to offer "pure vanilla" debentures and shares, therefore lifting restrictions on issuing securities to both retail and non-retail investors.[108] Indonesia enacted its ECF regulation in January 2019, the Equity Crowdfunding Rule, which requires providers to obtain a license.[109] Pursuant to the Capital Markets and Services Act 2007, the Securities Commission Malaysia released the Guidelines on Recognized Markets in December 2015, outlining regulations for ECF platforms that must register as recognized market operators (RMOs) in Malaysia.[110] Interestingly, in China crowdfunding still remains unregulated, The Securities Association of China proposed a set of draft regulations in 2014 that would impose restrictions on the activities of platforms, including barring them from raising funds on behalf of companies and from serving as investment advisors, but these have not yet been issued.[111]

Malaysia added peer-to-peer (P2P) lending platforms to the Guidelines on Recognized Markets in May 2016, followed by digital asset exchanges and property crowdfunding platforms.[112] These platforms must also register as recognized market operators (RMOs). As of June 2020, a total of ten equity crowdfunding (ECF) platforms, eleven P2P financing platforms, three digital-asset exchanges and a property crowdfunding platform have been registered with the regulator.[113] Although not conceived from the start, the Guidelines have become an overarching national regulatory framework for alternative finance, a type of "consolidated" framework for fintech. Indonesia introduced, in December 2016, a license for peer-to-peer (P2P) lending platforms,[114] and has since published periodically updated checklists for P2P lending platforms to adhere to.[115] In April 2019, the Bank of Thailand similarly issued a notification setting out the rules, procedures, and conditions for P2P lending businesses and platforms. Prior to this notification, the legal status of P2P

106. Simone Di Castri, GSMA, "Enabling Mobile Money Policies in Sri Lanka–The Rise of eZ Cash."
107. For more details on the China and P2P lending platforms, see the case study (box 5) in World Bank, Fintech Note No. 5, "How Regulators Respond to Fintech: Evaluating the Different Approaches–Sandboxes and Beyond."
108. Silk Legal, Thai SEC Clarifies Equity Crowdfunding Regulations.
109. Baker McKenzie, "Indonesia: OJK (Finally) Released Equity Crowdfunding Regulation."
110. Guidelines on Recognized Markets.
111. Griffin Davis, The Regulatory Review, "Regulation of the Chinese Equity Crowdfunding Market."
112. Guidelines on Recognized Markets, ibid.
113. Securities Commission Malaysia, List of Registered Recognized Market Operators.
114. Daniel Adriana and Wawan Dhewantoa, Journal of Internet Banking and Commerce. "Regulating P2P Lending in Indonesia: Lessons Learned from the Case of China and India."
115. Greita Anggraeni, "Peer-to-Peer Lending in Indonesia: A Regulatory Update."

lending activities in Thailand was not consistent or clear cut, with some types of P2P lending being strictly prohibited without a license from the BOT or the Securities and Exchange Commission of Thailand.[116]

Neither Indonesia nor Thailand have consolidated their regulations for alternative finance as is the case of Malaysia. Although Thailand initially considered implementing a fintech law, this was ultimately withdrawn. Its enactment might have implied that the prior Electronic Transaction Act was insufficient to validate electronic transactions, raising the question of whether additional legislation would be needed to support electronic transactions in other sectors.[117]

Selected Regulatory Strategies in Latin America and the Caribbean (LAC)

Despite relatively high mobile and internet penetration rates in the region, the adoption of mobile money services remains low due to high bankarization rates (on average, 53 percent of the population had an account at a financial institution in 2017, with over 73 percent in Venezuela, 70 percent in Brazil, and 68 percent in Costa Rica).[118] On the other hand, the growth of digital payments and digital banking is very strong,[119] and open banking regimes, which are premised on bank accounts, are proliferating in countries such as Mexico and Brazil. Most alternative financing in LAC is done through lending activities, rather than crowdfunding (IMF 2019). And in countries such as Argentina, Brazil, and Mexico, big tech firms such as Mercado Libre, offer a range of payment, lending, and wealth management services, growing quickly from a small base (FSB, 2020b).

In this context, regulators have focused on active regulatory reform, often through activity-based regulations, but there are barriers. These include rigid legal frameworks that limit the adoption of new technologies and take a long time to adapt, legal ambiguity, lack of clarity (or even nonexistence) of the regulatory frameworks, and inconsistencies among different regulations covering similar activities.[120] It is thus not surprising that according to the WB and CCAF Survey (2019), there is a relative absence of regulatory innovation facilitators in LAC, with only 8 percent of survey respondents based in the region offering or developing a regulatory sandbox (versus 32 percent in Africa).

There are, however, some bright spots. Uruguay, Argentina, and Bermuda have set up innovation hubs, while current regulatory sandboxes in the region include:

- Banco Central do Brazil's sandbox launched in February 2021[121]
- Bermuda's Insurance Regulatory sandbox since 2018[122]
- Barbados' Fintech Regulatory sandbox established by the Central Bank of Barbados and the Financial Services Commission in 2019[123]
- Bank of Jamaica's sandbox in 2020[124]
- CNBV and Banco do Mexico's sandbox set up under the Fintech Law.

Mexico's Fintech law, which regulates crowdfunding, EMIs, the use of cryptocurrency, and entities that offer "innovative models," is both a regional benchmark (World Bank and CCAF, 2019) for other regulators and a unique regulatory approach in the region in its attempt to create a "consolidated" regulatory framework for fintech activities to overcome issues created by its civil law mandate. (See box below) Chile is considering introducing a similarly broad fintech law with the publishing of

116. Conventus Law, "First Peer-to-Peer Lending Regulation Issued by the Bank of Thailand."
117. World Bank. "Thailand Background Note: Fintech."
118. World Bank, 2017 Global Findex Database.
119. CEMLA Fintech Forum, Fintech Regulatory Aspects Working Group. "Key Aspects around Financial Technologies and Regulation Policy Report,"
120. Ibid.
121. https://www.bcb.gov.br/estabilidadefinanceira/sandbox.
122. Bermuda Monetary Authority, "Guidance Note, Insurance Regulatory Sandbox and Innovation Hub."
123. See website of Central Bank of Barbados here.
124. Bank of Jamaica, "Fintech Regulatory Sandbox Guidelines."

a draft proposal in February 2021,[125] while a special congressional commission in Brazil is working on a broader legislative strategy for fintech activities, having individually legislated crowdfunding and P2P lending.[126]

Still the main trend is towards new specialized regulations that cover individual fintech activities, especially e-money, rather than having a consolidated law covering the whole array of activities. Several jurisdictions have acted (through different legal tools) to regulate fintech activities individually. These include Peru (Electronic Money Law in 2013), El Salvador (Law to Facilitate Financial Inclusion in 2019, which authorizes e-money and savings accounts with simplified requirements), Colombia (Act 1735/2014 regarding Specialist Electronic Payment and Deposit Companies in 2014), Paraguay (Regulation for Electronic Means of Payments in 2014), Brazil (Law 12.685 and BACEN Circulars in 2013 and 2014), and Jamaica (the 2013 Guidelines for Electronic Retail Payment Services, revised in 2019). With the exception of Colombia's recent equity crowdfunding regulation,[127] Uruguay's P2P lending regulation in 2018, and Brazil's individual regulations concerning crowdfunding and P2P lending, the regulation of alternative finance, however, has not been a top regulatory priority in the region. According to the WB CCAF Survey, a majority of regulators in LAC are willing to tolerate an unregulated but active alterative finance sector, with 65 percent of jurisdictions not regulating P2P lending, 58 percent not regulating equity crowdfunding, and 31 percent not regulating initial coin offerings in any form. However, there seems to be an appetite for regulatory change in the near future to increase financial inclusion and development: 81 percent of regulators in Latin America expect to make changes to their equity crowdfunding frameworks, with nearly half expecting to review the regulation of ICOs and 23 percent expecting to revise P2P lending regulations in the near future (World Bank and CCAF, 2019).

Mexico's Fintech Law

Mexico's Fintech Law has been heralded as an innovative approach to regulating fintech activities. By articulating a strategic framework covering several types of fintech, it has championed a "consolidated" approach that has differentiated it from most other jurisdictions, who have taken a more fragmented, piecemeal strategy when grappling with regulation of fintech activities. The main reason for Mexico's approach is its civil law tradition, which restricts regulators from regulating in areas and with tools that are not explicitly identified in the legislation that bestows their mandate (also known as "rule-based permission"). Mexican regulators were restricted in using risk proportionality and judgement-based supervision as tools to regulate fintech. In this context, the issuance of an omnibus fintech law allowed for a broad mandate for its financial sector regulators over certain areas and permitted their use of tools such as risk proportionality and innovation facilitators.

The main provisions of the Law are as follows:

- A licensing framework for the authorization, operation, and supervision of Financial Technology Institutions (FTIs), which include crowdfunding institutions (IFCs) and electronic payment funds institutions (IFPEs).
- The creation of a Regulatory Sandbox environment for companies with "novel models" that are outside the established regulatory perimeter.
- The introduction of an open banking regime, that is, mandatory data exchange between regulated financial institutions with consumers' consents through standardized Application Programming Interfaces (APIs).
- The recognition of virtual assets and regulation of their conditions, including restrictions of transactions and operations in Mexico.

Although conceptually an omnibus framework grouping several fintech activities was arguably an optimal response, especially given the institutional regulatory constraints faced by Mexico, the implementation of the law has been

125. Carey, CMF publishes Fintech Law Proposal.
126. Techcrunch, "Fintech Regulations in Latin America Could Fuel Growth or Freeze Out Startups."
127. Quarta, "Crowdfunding Regulation in Colombia: Boost or Limitation to Alternative Investment"

hampered by lack of political support and plagued with capacity constraints. Hence it has been subject to criticism.[128] As a consequence, the first licences for "Financial Technology Institutions were issued only in February 2021, despite 85 fintech firms having applied for it by September 2019—of which 60 are online payment processors and 25, crowdfunding platforms.[129] Currently many of these entities still continue to operate under transitional provisions of the Fintech Law, which gave fintech firms a year to conform to the Law. It appears this transitional period is being extended to accommodate for the lack of license issuance. Equally, in regard to open banking secondary legislation, although the CNBV was due to issue all secondary regulations by March 2020, only one set of regulations, relating to access of public data concerning ATMs, was in fact issued. The regulations concerning the implementation of open banking for open financial data on other financial products and service, aggregated statistical data on transactions, and consumer transactional data for products or services, will now be released at a later date, possibly in 2021.

Further industry stakeholders have criticized the requirements for such FTIs, saying they are too burdensome and disproportionate to the risks involved. Specifically, they argue that the capital requirements for crowdfunding are too high, and that there is a disparity in application of KYC/CDD requirements between FTIs and banks, with stricter requirements being imposed on the FTIs without justification of higher risk. Similarly, e-money providers have complained of the excessive burdens of the e-money requirements. This has led some prominent fintech providers such as PayPal to opt out of obtaining an FTI license, and to continue to operate as a payment aggregator, albeit with more limited functionality than an FTI.[130]

128. This is in part because after the passage of the law on March 9, 2018, a new government was voted into office on July 2, 2018. This government has been less interested in supporting fintech. Lack of experienced civil servants and staff reductions have handicapped the ability to implement provisions of the Fintech Law. More recently, some commentators, such as CGAP have argued that Mexico's Fintech law is actually a misnomer, in that it only covers two types of fintech companies, and does not provide regulatory guidance for other technology-enabled innovations in financial services, such as fintech firms offering balance-sheet lending, big tech companies launching financial services, investment services other than crowdfunding, or central bank digital currencies (Stefan Staschen and Mehmet Kerse, "Is Mexico's 'Fintech Law' Leading a New Trend in Fintech Regulation?").
129. Omar Faridi, Crowdfund Insider, "85 Fintech Firms have Submitted Applications to Operate in Mexico."
130. Ibid.

Bibliography

Appaya, M.S., Dohotaru, M., Ahn, B., Kliatskova,.T., Seshan, P. and Pascaru, I. 2020. "A Roadmap to suptech Solutions for Low Income (IDA) Countries." Fintech Note 7, World Bank.

Basel Committee on Banking Supervision. 2018. "Sound Practices Implications of Fintech Developments for Banks and Bank Supervisors."

Basel Committee on Banking Supervision. 2016. "Guidance on the Application of the Core Principles for Effective Banking Supervision to the Regulation and Supervision of Institutions Relevant to Financial Inclusion."

Bolzico, J., Mascaró, Y. and Granata, P. 2007. "Practical Guidelines for Effective Bank Resolution." World Bank Policy Research Working Paper 4389.

Carletti, E., S. Claessens, A. Fatas, and X. Vives. 2020. "The Bank Business Model in the post-Covid-19 World." The Future of Banking, CEPR Press.

Castanier, M., Roussely, B. 2018. "Revue Banque, Intégrer le Risque Cyber dans la Gouvernance des Risques Bancaires."

Centro de Estudios Monetarios Latinoamericanos. 2019. "Key Aspects around Financial Technologies and Regulation Policy Report."

Chatain, P.L., Zerzan, A., Noor, W., Dannaoui, N., de Koker, L. 2011. "Protecting Mobile Money against Financial Crime: Global Policy Challenges and Solutions."

Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions. 2016. "Guidance on Cyber Resilience for Financial Market Infrastructures."

Crisanto, J.C., Ehrentraud, J. 2021. "The Big Tech Risk in Finance." IMF blogs.

Dias, D. 2020. "Cloud Computing: Issues for Supervisors," Toronto Centre Notes.

Dias, D., Staschen, S. 2018. "A Guide to Supervising E-Money Issuers." CGAP.

di Castri, Simone and Grasser, Matt and Kulenkampff, Arend. 2020. "The 'DataStack': A Data and Tech Blueprint for Financial Supervision, Innovation, and the Data Commons." BFA Global.

European Banking Authority. 2019. "Guidelines on Outsourcing Arrangements."

Feyen, E., Frost, J., Natarajan, H., Saal, M. 2021. "Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Competition." (Market Structure note). BIS Working Paper and World Bank Group Fintech and the Future of Finance Technical Note.

Financial Action Task Force. 2019, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers."

Financial Stability Board. 2020a. "Regulation, Supervision, and Oversight of Global Stablecoin Arrangements."

Financial Stability Board. 2020b. "BigTech Firms in EMDEs: Market Developments and Potential Financial Stability Implications."

Financial Stability Board. 2020c. "Effective Practices for Cyber Incident Response and Recovery: Final Report."

Financial Stability Board. 2020d. "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion Paper."

Financial Stability Board. 2019a. "BigTech in Finance: Market Developments and Potential Financial Stability Implications."

Financial Stability Board. 2019b. "Regulatory Issues of Stablecoins."

Financial Stability Board. 2019c. "Fintech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications."

Financial Stability Board. 2017a. "Financial Stability Implications from Fintech."

Financial Stability Board. 2017b. "Summary Report on Financial Sector Cybersecurity Regulations, Guidance, and Supervisory Practices."

Financial Stability Board. 2014. "Key Attributes of Effective Resolution Regimes for Financial Institutions."

Financial Stability Institute. 2021. "The Universe of Supervisory Mandates—Total Eclipse of the Core?" FSI Insights on Policy Implementation No. 30.

Financial Stability Institute. 2020. Policy Responses to Fintech: a Cross-Country Overview." FSI Insights on Policy Implementation No. 23.

Financial Stability Institute. 2017. "Regulatory Approaches to Enhance Banks' Cybersecurity Frameworks." FSI Insights on Policy Implementation No. 2.

Frost, J. 2020. "The Economic Forces Driving Fintech Adoption across Countries." BIS Working Paper No. 838.

G7. 2016. "G7 Fundamental Elements of Cybersecurity for the Financial Sector."

Izaguirre, J.C., McGuire, C., Grace, D. 2015. "Deposit Insurance for Digital Financial Products: 3 Approaches." CGAP.

Izaguirre, J.C., Dias, D., Kerse, M. 2019. "Deposit Insurance Treatment of E-Money: An Analysis of Policy Choices." CGAP Technical Note.

International Monetary Fund and the World Bank Group. 2019. "Fintech: the Experience So Far."

International Monetary Fund and the World Bank Group. 2018. "The Bali Fintech Agenda: a Blueprint for Successfully Harnessing Fintech's Opportunities."

International Monetary Fund. 2020. "Institutional Arrangements for Fintech Regulation and Supervision." Note 19/02.

Padilla, A.J. 2020. BigTech "Banks", Financial Stability and Regulation. Revista de Estabilidad Financiera, Núm. 38. Banco de España.

Pazarbasioglu, C., Garcia Mora, A., Uttamchandani, M., Natarajan, H., Feyen, E.; Saal, M. 2020. "Digital Financial Services." World Bank.

Pereira da Silva, L. 2018. "Fintech in EMEs: Blessing or Curse?" Bank for International Settlements.

Philippon, T. 2016. The Fintech Opportunity. NBER Working Paper No. 22476.

Philippon, T. 2019. "On Fintech and Financial Inclusion." NBER Working Paper No. 26330,

Plaitakis, A. Staschen, S. 2020. "Open Banking: How to Design for Financial Inclusion." Working Paper. Washington, D.C., CGAP

Plaitakis, A., Soursourian, M. 2019. "Fair Play: Ensuring Competition in Digital Financial Services." Working Paper. Washington, D.C., CGAP

Plaitakis, A., Kirk, T., and Church, B. 2016. ADB Technical Assistance Consultant's Report, "'Regional: Promoting Remittance for Development Finance. Digital Payment Systems, Mobile Money Services, and Agent Banking: Bangladesh, Nepal, and Sri Lanka."

Restoy, F. 2021. "Financial Regulation: How to Achieve a Level Playing Field." Financial Stability Institute Occasional Paper, Bank of International Settlements

Staschen, S., Kerse, M. 2021. "Is Mexico's "Fintech Law" Leading a New Trend in Fintech Regulation?"

Toronto Centre. 2017. "Fintech, Regtech, and Suptech: What They Mean for Financial Supervision."

Toronto Centre. 2018. " Ssuptech: Leveraging Technology for Better Supervision."

Toronto Centre. 2019. "Supervising Fintech and Promote Financial Inclusion."

UNSGSA Fintech Working Group and CCAF. 2019. "Early Lessons on Regulatory Innovations to Enable Inclusive Fintech: Innovation Offices, Regulatory Sandboxes, and Regtech." Report.

Vives, X. 2019. "Digital Disruption in Banking." Annual Review of Financial Economics, Vol. 11, pp. 243-272

World Bank. 2020a. "How Regulators Respond To Fintech: Evaluating the Different Approaches—Sandboxes and Beyond." Fintech Note No. 4.

World Bank. 2020b. "Berg, G., Guadamillas, M., Natarajan, H., Sarkar, A. 2020. "Fintech in Europe and Central Asia: Maximizing Benefits and Managing Risks." Fintech Note, No. 4.

World Bank. 2019. "Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit, and Deposits."

World Bank. 2018. "From Spreadsheets to Suptech Technology Solutions for Market Conduct Supervision."

World Bank and Cambridge Centre for Alternative Finance. 2019. "Regulating Alternative Finance: Results from a Global Regulator Survey."


WORLD BANK GROUP