NO. 245

MAY
2023

ADB BRIEFS

KEY POINTS

- Regulatory authorities need to adjust regulations to adapt to emergent financial technology (fintech) providers, products, and services as the fintech sector is developing rapidly, spurred by the coronavirus disease pandemic.
- Updated and flexible licensing, regulation, and oversight of fintech providers are needed to minimize fintech-related risks.
- To keep pace, regulatory sandboxes and innovation offices allow regulators to stay on top of developments and existing regulations.
- Regulators must continue to create new skills, capabilities, and organizational culture that values and encourages innovation. New developments in regulatory technologies (regtech) and supervisory technologies (suptech) are also helping.
- Addressing new fintech risks also means ensuring that financial consumer protection regulations are updated to cover financial and operational issues, greater connectivity, weak internal control and oversight systems, cybersecurity, and consumer risks.
- National and international regulatory coordination are key to better manage fintech risks.

ISBN 978-92-9270-153-6 (print)
ISBN 978-92-9270-154-3 (electronic)
ISSN 2071-7202 (print)
ISSN 2218-2675 (electronic)
Publication Stock No. BRF230170-2
DOI: http://dx.doi.org/10.22617/BRF230170-2

Managing Fintech Risks: Policy and Regulatory Implications

Yonghwi Kwon
Financial Sector Specialist
Finance Sector Group
Asian Development Bank

John Owens
Senior Digital Finance Advisor
Digital Finance Advisory Services

Jae-Deuk Lee
Head of e-Business Strategy Team
Korea Financial Telecommunications and Clearings Institute

INTRODUCTION

Financial technology (fintech) development has spread rapidly around the world, especially in the last few years, amid new regulatory policies and the now-waning coronavirus disease (COVID-19) pandemic. This is lowering transaction costs, boosting the variety of financial services, and expanding access and financial inclusion in markets.[1]

Yet, risk management and mitigation demands have risen alongside the increasing use of fintech products and services and the growing number of financial players and providers. Given the variety of developments in different markets, financial regulators have responded in likewise diverse ways, while financial standard-setting bodies have tried to coordinate and develop new global standards for regulators and policy makers, especially for managing fintech risks.[2] These fintech risks include financial risks, operational risks,[3] cybersecurity risk, and risks to consumers.

Notes: In this publication, "$" refers to United States dollars.
ADB recognizes "China" as the People's Republic of China and "Korea" as the Republic of Korea.

[1] The authors would like to thank Junkyu Lee, chief of the Finance Sector Group and Peter Rosenkranz, financial sector specialist for their valuable comments and inputs to the brief; Eric Van Zant as editor; and Katherine Mitzi Co and Matilde Cauinian from the ADB Finance Sector Group for their valuable administrative support.

[2] Especially the Basel Committee on Banking Supervision, the Committee on the Global Financial System, the Committee on Payments and Market Infrastructures, the Financial Action Task Force, the International Association of Deposit Insurers, the International Association of Insurance Supervisors, the International Monetary Fund, the International Organization of Securities Commissions, the Islamic Financial Services Board, the Organisation for Economic Co-operation and Development, and the World Bank.

[3] These operational risks include insufficient operational capacity, the risks of greater connectivity, the risk of weak internal control and oversight systems.

ADB

This policy brief focuses on policy and regulatory considerations for managing the risks associated with fintech.

While many traditional financial service providers are adopting fintech, a whole new range of fintech providers are entering the market and offering services directly to customers. These entrants are generally smaller than traditional financial service providers and often interact with customers digitally. Authorities need to adjust existing financial policies and regulations and create new ones to provide appropriate oversight and supervision of the emerging new providers.

In its focus on risks in the fintech sector, the brief also recommends actions policy makers and regulators could take to better manage risks as products and services spread.

THE EVOLVING FINTECH LANDSCAPE

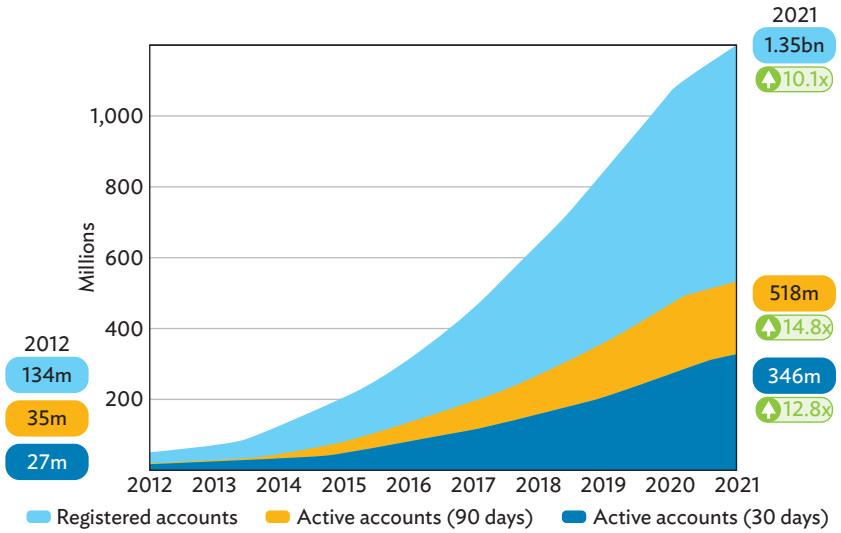
The Rapid Growth of Fintech

Advances in Big Tech, fintech, and mobile financial services. The Financial Stability Board (FSB) defines fintech as "technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services."[4] This definition includes new fintech providers as well as existing financial institutions utilizing new innovative digital financial services. Adopting rapidly developing information and communication technologies into existing services, financial institutions have continuously improved digital banking and payment as well as other financial services. New players have grown rapidly during the COVID-19 pandemic, especially Big Tech firms and particularly in the e-commerce field and payments including fintech mobile payment applications (Figure 1).

In a few markets, fintech applications, especially digital payments, grew dramatically during the COVID-19 pandemic. In Cambodia, digital e-wallet accounts, including those offered by banks, grew from 4 million at the end of June 2019 to 17.9 million by December 2022, with most of the rapid growth as the COVID-19 pandemic hit and lockdowns occurred.

Given Cambodia's population of fewer than 17 million people, the impact of these numbers on widening financial inclusion was significant. Along with the development and use of a standardized quick response (QR) code known as KHQR, 37 banks and payment services providers were able to reach out to more than 230,000 small shops and merchants by 2022. This trend also helped leapfrog the number of digital payment transactions, from 68.8 million in the first half of 2019 (combined United States [US] dollar and Cambodian riel transactions) to 182.39 million in the first half of 2022. Even more surprising was the dramatic increase in mobile banking transactions—from only 14.83 million in the first half of 2019 to more than 205.59 million in the first half of 2022. Table presents this increase by value.

Figure 1: Number of Registered and Active Mobile Money Accounts, 2012–2021



bn = billion, m = million.

Source: GSMA State of the Industry Report on Mobile Money 2022. https://www.gsma.com/sotir/wp-content/uploads/2022/03/GSMA_State_of_the_Industry_2022_English.pdf.

[4] FSB. 2017. *Financial Stability Implications from Fintech: Supervisory and Regulatory Issues that Merit Authorities' Attention*. Basel: FSB.

Table: Number of Digital Transactions in Cambodia
(millions)

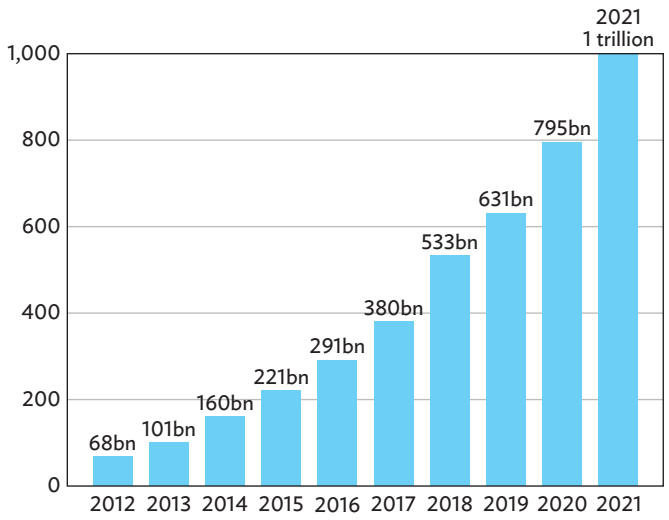
	Mobile Banking Transactions		Mobile Payments (payment service institutions and banks)	
Timeframe	KHR	USD	KHR	USD
H1 – 2019	0.56	14.27	24.40	39.40
H2 – 2019	0.96	26.21	30.30	48.30
H1 – 2020	14.35	40.87	35.01	52.89
H2 – 2020	3.90	63.17	49.98	62.58
H1 – 2021	4.58	96.10	54.66	67.09
H2 – 2021	7.62	145.83	68.73	94.39
H1 – 2022	12.21	193.38	77.31	105.08

H = half, KHR = Cambodian riel, USD = United States dollar.

Note: Similar trends also occurred in markets as diverse as Indonesia and the Philippines, where Big Tech firms like GoJek in Indonesia and telecom firms Globe and Smart Communications in the Philippines facilitated rapid e-money adoption.

Source: Payments Department National Bank of Cambodia.

Figure 2: Total Annual Value of Global Mobile Money Transactions, 2012–2022 ($)



bn = billion.

Source: GSMA State of the Industry Report on Mobile Money 2022. https://www.gsma.com/sotir/wp-content/uploads/2022/03/GSMA_State_of_the_Industry_2022_English.pdf.

New policy and regulatory developments. Rapid fintech growth has also been supported by changes in regulatory policies, especially more flexible electronic know-your-customer (KYC) regulations and changes to contactless transaction limits. KYC regulations are in place to generally manage anti-money laundering and combating the financing of terrorism (AML/CFT) to meet Financial Action Task Force (FATF) guidelines. After lobbying from several emerging markets, the FATF did issue new guidelines to allow tiered KYC regulations as well as tiered transaction limits to allow low-value, low-risk transactions for such things as e-money services.[5] During the COVID-19 pandemic, several jurisdictions allowed more flexible KYC requirements as well as increased transaction limits. This resulted in an overall increase in users and transactions during the COVID-19 pandemic (Figure 2).

Driven in large part by the pandemic, policy makers and financial regulators have worked to increase access and the openness of financial systems to ensure that more innovative fintechs can seamlessly enter the market and compete on a level playing field. In addition, authorities are moving to introduce flexible regulatory regimes to facilitate adoption of new financial services in line with legal frameworks.[6]

Because existing regulations fail to meet the fast-paced market changes, fintechs have unleashed through their innovative financial services. Countries have increasingly introduced regulatory sandboxes in markets including Indonesia, Malaysia, and Thailand and the test-and-learn approach in markets like Cambodia and the Philippines to stay on top of developments. Sandboxes can help prevent fintech companies' innovative activity from being aborted or delayed by existing regulation; for instance, by allowing fintech companies to release their financial offerings in the market without having to obtain financial business permits or licenses as long as they are within limited boundaries (in number of users, service duration, etc.).

Open banking refers to a method or system that enables a third-party service provider to safely and efficiently access customer financial data held by banks via Application Programming Interface (API).[7] Its openness facilitates web services and application development by enabling efficient use of services, information, and data held by businesses. For this reason, it has been deemed an appropriate means to provide fintech services that connect banks and nonbanking institutions. As such, voluntary initiatives, such as the "Open Banking Project" were introduced in several markets.[8]

[5] For information, see the Financial Action Task Force at https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf.
[6] Regulatory sandboxes and open banking regulations, such as the European Union's Payment Services Directive 2 (PSD2), are the leading examples.
[7] API refers to interfaces that allow application programs to be written based on an operating system, application, library, etc.
[8] As distrust in large financial institutions grew after the global financial crisis in 2007 and 2008, groups of developers led continuous efforts to improve financial transparency by creating open API settings. A leading example is the open banking project, launched in 2013 by Germany's Technology Solution Berlin (known as TESOBE).

The New Fintech Landscape

Fintech services were developed early in the payment services sector, where entry into financial services and securing customers was easier. A large untapped customer base not served by traditional banks also helped create a huge opportunity.[9] Over time, fintechs began to provide digital credit services, personal asset management, robo-advisory services, and then a range of digital versions of traditional financial products and services such as digital savings and insurance mostly through partnerships (Figure 3).

Fintech Risks to the Financial System

As the fintech landscape rapidly expands, risks are developing that policy makers and regulators need to address.

Figure 3: Fintech Services

Source: Authors.

[9] This was most prominent in emerging markets in Asia and Africa, where e-money initiatives took off, but also in markets such as the US and the People's Republic of China where e-money services such as PayPal and AliPay grew rapidly.

Financial Risks

Financial risks in the fintech industry depend on the size and scale of the fintech operation. These can be broadly defined as credit or liquidity risks that may result in bankruptcy or business closure. Regulatory and policy environments are also adapting tiered approaches to address financial risks, which can be based on the size and volume of the fintech player.[10] These approaches include developing an understanding of new fintech players, products and services, and learning from the experiences in other jurisdictions. Financial services regulatory authorities need to regulate firms that accept and manage money for others, especially in the payment industry, and these firms should follow international standards in safeguarding customer funds (escrow and trust account rules). In addition, minimum capital requirements for fintechs need crafting, depending on the markets, but should be sufficient to cover potential risks.[11] For example, in the People's Republic of China (PRC), where large e-money operators such as Alipay and Tenpay flourish, stringent regulations require operators to increase the payment reserve ratio to 100%, ultimately to become regulated financial institutions.[12]

Operational Risks

Generally, operational risk is defined as "the risk that deficiencies in information systems or internal processes, human error, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services."[13] A wide range of operational risks can occur during business operations. Fintech also has potential operational risks, such as:

Insufficient information technology infrastructure and operational capacity. Many nonbank fintech firms focus more on innovative technologies that increase speed. These require firms to adapt processes to ensure stability, reduce fraud, manage data, and regulatory compliance, but some firms, especially smaller firms, have fallen short of expectations. The main challenge for many fintech firms is to deal with the speed of industry change, which is often rapid. The FSB also highlights the operational risks associated with the lack of effective governance or process control which can lead to the disruption of financial services or critical information technology (IT) infrastructure.[14]

Unanticipated market events are another major operational risk that can be exacerbated by poor operational controls. Weak IT infrastructure and operational capacity, for example, undermined US fintech and online trading app Robinhood during the GameStop stock frenzy.[15]

Increased interconnectivity risks. To reduce IT infrastructure-related costs, many fintech companies are connecting with third-party services such as cloud computing and data services or tapping into various APIs or solutions provided by banks or other operators. However, this interconnectivity can also cause related risks to other financial service providers.[16] For example, a major US fintech's relatively recent service disruption was caused by inadequate processing capacity stemming from an excessive increase in workload and technical issues in accessing third party service providers (Box 1).[17]

Box 1: A Major United States Fintech's Service Disruption: The Neobank, Chime, in 2019

The neobank Chime had grown rapidly since its establishment in 2013 and, as of October 2019, had reportedly managed more than 5 million customer accounts. However, a 2-day outage from 16 October 2019 significantly interfered with the popular American neobank's core operations. Chime's website and mobile app went down and Chime card transactions and cash withdrawal services were disabled. The company said the disruption was due to technical difficulties in Galileo Financial, its payment processing third party service provider. The service was restored later, but it could not avoid customer complaints.

Source: Gregory Magana. 2019. US Neobank Chime Suffers Major Outage. *Business Insider*. 21 October.

[10] In several jurisdictions, fintech licensing requirements are tiered to consider financial risks. In Japan, payment service providers are based on the maximum value they can execute. Capital requirements may also be tiered; for example, e-money providers have set bands of capital as a percentage of their e-money float (usually 2%–5%) (see J. Ehrentraud, J. Prenio, C. Boar, M. Janfils, and A. Lawson. 2021. Fintech and Payments: Regulating Digital Payment Services and E-Money. *FSI Insights on Policy Implementation*. No. 33. Bank for International Settlements, Basel. https://www.bis.org/fsi/publ/insights33.pdf).

[11] For instance, in the Republic of Korea, Electronic Banking Supervision Regulation Article 63 (Prudential Management Guidelines for Electronic Financial Business Operators) clearly states that the ratio of equity capital to outstanding unpaid amounts shall be 20/100 or more for electronic currency and prepaid electronic payment means, while the ratio of assets with low investment risk to total assets shall be at least 10/100.

[12] In 2017, the People's Bank of China (PBOC) tightened control over reserve funds of the country's third party payment service providers, including Alipay. These included (i) increasing the reserve requirement ratio to 100%; (ii) requiring reserve funds in commercial bank accounts to be held in the PBOC's reserve account and shortening the pay period from quarterly to monthly; and (iii) requiring all electronic payments to be processed via integrated payment platform, known as NetUnion Clearing Corporation (Wang'lian). See KIF. 2018. Financial Risk Control Measures in the PRC's Digital Payment Market.

[13] Bank for International Settlements (BIS). Principles for Financial Market Infrastructures. Basel. https://www.bis.org/cpmi/info_pfmi.htm.

[14] Financial stability implications from FSB (2017).

[15] Jennifer Tescher. 2021. The GameStop Stock Frenzy Is Turning Into A Cautionary Tale for FinTech. *Forbes*. 1 February. https://www.forbes.com/sites/jennifertescher/2021/02/01/the-gamestop-stock-frenzy-is-turning-into-a-cautionary-tale-for-fintech/?sh=2c7727914877.

[16] See A. Khan and M. Malaika. 2021. Central Bank Risk Management, Fintech, and Cybersecurity. *IMF Working Paper*. No. 2021/105. Washington, DC: IMF.

[17] The 10 biggest fintech companies in the US in 2020 as per Forbes were (i) Stripe (payments), (ii) Ripple (blockchain and Bitcoin), (iii) Coinbase (blockchain and Bitcoin), (iv) Robinhood (trading), (v) Chime (personal finance), (vi) Plaid (payments), (vii) SoFi (personal finance), (viii) Credit Karma (personal finance), (ix) Opendoor (real estate), and (x) Root (insurance). See J. Kauflin. 2020. The 10 Biggest Fintech Companies in America. *Forbes* . 12 February.

These interconnectivity operational risks can become more prominent in open banking and open finance ecosystems. The complexity of open banking and, now, open finance environments,[18] can create unique challenges, especially in cross-border situations where each country may have distinct systems and different regulations. In a country where the regulation allows banks autonomy in providing open banking system access to fintechs or with no standardized systems yet, fintechs may strike an agreement with each and every bank to use APIs or provide services in nonstandard ways, such as screen scraping.[19]

Weak internal control and oversight systems. The essence of the fintech market is the emergence of new and innovative services that enhance or introduce new financial products and services. In several markets, early fintech providers often started outside established financial regulatory frameworks or in test-and-learn[20] or wait-and-see[21] regulatory environments. For instance, across many countries, crypto-asset transactions were carried out or used as money transfer services for years prior to the defining virtual asset service provider regulations.

Service providers operating outside the regulatory framework are generally subject to less stringent supervision and oversight than incumbent financial institutions. To some extent, this is necessary to encourage the growth of fintech and financial innovation, but this regulatory flexibility requires constant monitoring to avoid risks, especially to consumers. Where no minimum standards or guidelines related to new types of fintech services exist, risk is higher that firms will not have appropriate internal controls in place. This can lead to an inadequate monitoring system and errors, failures, or even fraud.

Examples of issues related to weak internal controls have demonstrated the impact this can have on unregulated fintech players, such as those providing decentralized finance[22] products and services, crypto asset services, or fintech-enabled online lending (Box 2).

Box 2: Lending Club Scandal

The Lending Club, established in 2007, has become the United States' largest peer-to-peer lending platform. Yet, due to weak internal controls, Lending Club discovered $22 million worth of loans that did not meet its standard minimum criteria, and were sold to an investor. It was also revealed that management turned a blind eye to employees falsifying documents. After an internal investigation, the firm acknowledged material weaknesses in its internal controls over financial reporting and stressed that it would work to improve them. Some members of the board of directors and the Chief Executive Officer either immediately resigned or were laid off. Shares of Lending Club plummeted, and the company lost market confidence, harming the overall reputation of the country's peer-to-peer lending market.

Sources: Roger Yu. 2016. Lending Club CEO Resigns After Loan Sales Probe, Shares Plummet. *USA Today.* 9 May; Hugh Son. Lending Club Buys Radius Bank in First Fintech Takeover of a Bank. *CNBC*. 18 February.

Cybersecurity Risks

Cybersecurity risk refers to risks particularly caused by cyber threats and attacks; in digital financial services such risks need to be continuously monitored and closely controlled,[23] since they can degrade trust and the reputation of financial services, not to mention their direct impact on secure transactions. This is even more important in the fintech industry, which is often dominated by smaller firms. The top cybersecurity-related risks for fintechs include malware, identity theft, data breaches, denial of service and "man-in-the-middle" attacks, integration loopholes, phishing attacks, and insider threats.[24] Mobile payment users

[18] An open banking model can have a wide range of third-party arrangements. Such arrangements might include fintech firms directly servicing consumers and intermediary data aggregator firms. They may also include other parties without contractual relationships with banks. Likewise, non-contracted entities authorized or licensed by certain authorities may be among third parties. In countries without defined open banking frameworks, it can be a challenge to set specific requirements or expectations for third parties. This is because contracts with banks or other regulatory controls are absent. It is also possible that, without a bank's knowledge, third parties are able to partner and share customer-permissioned data from banks with fourth parties. See BIS. 2019. *Report on Open Banking and Application Programming Interfaces.* Basel: BIS. https://www.bis.org/bcbs/publ/d486.htm.

[19] *Fintech Times.* 2022. Nordigen: Screen Scraping as a Cybersecurity Risk Can Lead to Virtual Chernobyl. 30 January. https://thefintechtimes.com/nordigen-screen-scraping-as-a-cybersecurity-risk-can-lead-to-virtual-chernobyl/.

[20] Financial Services Regulatory Authority of Ontario. 2022. Test and Learn Environments for Financial Services Innovation. Toronto. https://www.fsrao.ca/media/5196/download.

[21] Wait-and-see regulatory oversight approaches have been practiced in a number of jurisdictions for crypto-assets, distributed ledger technologies, and peer-to-peer lending and crowdfunding. See World Bank. 2020. How Regulators Respond to Fintech Evaluating the Different Approaches—Sandboxes and Beyond. *Finance, Competitiveness & Innovation Global Practice Fintech Note.* No. 5. https://documents1.worldbank.org/curated/en/579101587660589857/pdf/How-Regulators-Respond-To-FinTech-Evaluating-the-Different-Approaches-Sandboxes-and-Beyond.pdf.

[22] R. Auer et al. 2023. The Technology of Decentralized Finance. Basel. *BIS Working Papers.* No. 1066. Harvard Kennedy School, Mossavar-Rahmani Center for Business and Government. https://www.bis.org/publ/work1066.htm. Using distributed ledger technologies, decentralized finance builds and offers services without using a traditional centralized intermediary. Such services may include trading, lending, smart contracts, investing, and the like. That decentralized finance components are programmable and may facilitate competitive financial markets. This may increase efficiency. Nonetheless, alongside decentralized finance comes huge technological and economic complexity. This complicates the assessment of risks and the potential of the associated financial products. Financial institutions and regulators need to systematically evaluate these factors.

[23] Cyber risk means the probability of a cyber incident and related ramifications, while a cyber incident includes all situations that can be caused by natural hazards, system disruption, cyber threat, and attack.

[24] In a "man-in-the-middle attack," parties position themselves in conversations between users and an application, doing so to either eavesdrop on or impersonate one of the parties.

have increasingly fallen victim to a variety of cybersecurity crimes. Venmo, a popular US mobile payment app owned by PayPal, has seen numerous cybersecurity risks that continue to affect clients including text scams, fake businesses, as well as in-person scams.

In the latest financial service business model, incumbent financial institutions are intertwined with different stakeholders and dependence on third-party fintech firms is steadily increasing. To address cybersecurity risks in a complex finance sector, systematic and holistic approaches are important. These include understanding and identifying stakeholders, their roles, and connections between each of them.

From a cybersecurity perspective, digital financial infrastructure is a prime target for attackers, primarily because its financial rewards are potentially high. Attackers' access to financial infrastructure has also increased amid the wide range of fintech players and the interconnectedness of the market.

Given concerns about cybersecurity risks, the European Systemic Risk Board published a report in 2020 on the subject to guide policy makers and regulators to better understand cyber threats, vulnerabilities, and the potential impact of an attack on a finance sector, with a step-by-step approach based on the conceptual systemic cyber risk model used to tackle this risk.[25]

Risks to Consumers

Additional fintech-related risks to consumers include issues of improper product design and delivery risks (especially via the mobile channel); in terms of digital lending, increased potential of overindebtedness; in the case of peer-to-peer lending, lack of transparency for clients and small investors; unfair treatment of marketing; data use and privacy; weak consumer complaint and redress mechanisms; and fraud.[26] Fintech providers collect extensive data on customers, including access to their financial transactional histories, mobile phone data including calls, SMS logs, contact lists, and photos geo-tracking of clients' locational histories. Some firms require access to or track social media accounts. Banks and fintech firms often view client data that they collect as *their* data which can be used and analyzed, while governments, such as the European Union, have long argued that the data is the *clients*' and they should have control over what is collected, how it is used, for what purpose, which parties have access to that data, and for how long the data can be stored.[27]

LESSONS FROM THE CASES OF MANAGING FINTECH RISKS

People's Republic of China

The PRC experience illustrates the need for guidance and requirements to mitigate fintech risks and protect consumers. In January 2022, the People's Bank of China (PBOC) unveiled its updated Fintech Development Plan 2022–2025,[28] which set out guidelines on the country's fintech development in the new era and set development goals, key tasks, and the implementation measures for digital transformation of the finance sector, which includes various measures to address risks. The guidelines suggest the following (footnote 28):

(i) Strengthen fintech governance, develop digital capabilities, and improve the financial technology ethics system featuring multiparty participation and collaborative governance, to build a digital ecosystem that promotes mutual progress.
(ii) Enhance data capability, promote orderly sharing, and comprehensive application of data on the premise of ensuring security and privacy, fully activate the potential of data as a factor of production, and effectively improve the quality and efficiency of financial services.
(iii) Improve the system for safe and efficient fintech innovation; build an operation middle platform that integrates business, technology, and data; establish an intelligent risk control mechanism; and fully activate new momentum for digital operations.
(iv) Speed up the all-round application of regulatory technology, strengthen the capacity building for digital regulation, implement closer supervision over fintech innovation, and build a firewall for finance and technology to fend-off risks.
(v) Cultivate fintech talent, refine relevant standards and rules, strengthen implementation of laws and regulations, and safeguard steady fintech development for the long run.

The PBOC also designed and implemented regulatory measures to control risk related to exponential growth of fintech payment services driven by Alipay and Tenpay. It also did this, in particular, to reduce the liquidity risk of funds that customers had previously deposited in their accounts held by payment service providers, such as Alipay, and to prevent an operator from managing high-risk funds, it increased the control over the funds. This included raising

[25] European Systemic Risk Board. 2020. *European Systemic Risk.* Frankfurt. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf?fdefe8436b08c6881d492960ffc7f3a9.

[26] J. A. Barefoot. 2020. Digital Technology Risks for Finance: Dangers Embedded in Fintech and Regtech. *M-RCBG Associate Working Paper Series*. No. 151. https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_151_final.pdf; and J. Owens. 2018. *Responsible Digital Credit*. Center for Financial Inclusion. https://www.centerforfinancialinclusion.org/responsible-digital-credit.

[27] While the European Union's (EU) General Data Protection Regulation is clear how client data can be accessed, used, and handled, cultural and political differences exist across different jurisdictions, and several emerging market countries still lack data protection laws and regulations.

[28] Regulatory News. 2022. PBC Sets Out Fintech Development Plan for 2022 to 2025. *Moody's Analytics*. 4 January. https://www.moodysanalytics.com/regulatory-news/jan-04-22-pbc-sets-out-fintech-development-plan-for-2022-to-2025.

the reserve requirement ratio to 100%, depositing reserve funds in a dedicated account at the PBOC, and payment processing via a comprehensive payment platform, NetUnion Clearing Corporation.[29]

Republic of Korea

The country's fintech development demonstrates the power of the regulatory sandbox to help regulators enhance regulations on fintech risks while promoting fintech development. With the enforcement of the Special Act on Financial Innovation Support in April 2019, the Financial Services Commission (FSC) announced its plans for a financial regulatory sandbox to promote the fintech industry. The Republic of Korea's sandbox supports the emergence of innovative financial services while monitoring its impact on consumers and the market to provide opportunities to implement regulatory reforms. In 2019, the FSC also introduced a standardized open API platform to ensure stable operation and risk management of open banking.

In July 2020, the FSC announced "Plans to Promote Digital Finance," which serves as a basis for financial service innovation and contains amendments of essential fintech-related regulations (including the Electronic Financial Transactions Act, etc.) to improve market credibility and stability. In January 2021, the FSC announced additional measures to support and manage fintechs. It focused on supporting the fintech industry through a regulatory sandbox, proposed legislation to nurture fintechs, and efforts to boost organizational capacity to support the fintech industry through relevant divisions and agencies. In addition, the FSC announced plans to promote online-based financial services, especially in big data analytics, mobile and online security and authentication, an enabling environment for network separation, management of links between fintechs and banks, and stable operation of open banking services. The FSC also supported the establishment of digital financial infrastructure, including rules on data privacy, protection and consumer rights, and infrastructure to support easy access to data convergence, and promoted appropriate infrastructure to enable artificial intelligence-based financial services.[30]

The FSC has been working to establish laws and regulations on digital assets for consumer protection and establishment of market order. In August 2022, the "Private–Public Task Force for Digital Assets" was launched and enactment of "Basic Act on Digital Assets" is under way.

Singapore

Singapore's experience includes lessons in balancing the important role that regulators can play in providing an appropriate enabling environment that supports innovation while ensuring safety and soundness measures. The Monetary Authority of Singapore (MAS) manages its dual role of supporting an enabling regulatory environment while also ensuring safety and security principles to facilitate the responsible development of the fintech industry. MAS's philosophy is that regulation should not get in the way of innovation but should carefully enable as well as monitor new financial technology products and services and continually evaluate the need to regulate them. Regulations are introduced when risks arising from innovative products and services cross a threshold or become material enough, with regulation being risk proportionate.[31]

MAS was also early in establishing a FinTech Regulatory Sandbox for new fintechs and established financial institutions to promote and facilitate testing of innovative fintech products and services. In addition, MAS used "softer" regulatory instruments including interpretative guidance on the application of existing laws and regulations on fintech solutions. These included guidelines that encouraged financial players to address new technology risks. Examples include the e-Payments User Protection Guidelines[32] and notices on technology and risk management practices related to outsourcing to third parties (such as cloud computing services).[33] MAS also worked to support and introduce the Payment Services Act in 2019.[34] This supported risk-specific legislation for payment-related services. That consolidated existing payment regulations and strengthened the role of MAS in overseeing new types of payment service providers.

European Union

The European Union (EU) experience highlights the important role for regional cooperation, especially in developing standards for open banking and data privacy. The EU's fintech regimes explained in the revised Payment Services Directive 2 (PSD2)[35] and the General Data Protection Regulation[36] are key to major EU member countries fintech policies. PSD2, in particular, presents ways to enhance consumer protection and transaction transparency while promoting fintech growth across Europe. The PSD2 defines roles and responsibilities of the payment initiation service provider and account information service provider and lays the foundation for fintech companies to access customer data and enter into various payment service markets.[37]

[29] Previously, payment service providers were able to split customer deposits in multiple commercial banks.
[30] See FSC. 2021. Financial Services Commission Announces Specific Plans for Financial Innovation and Digital Finance. https://www.fsc.go.kr/eng/pr010101/75260.
[31] MAS. 2016. Singapore's FinTech Journey – Where We Are, What Is Next. Speech by Ravi Menon, Managing Director, MAS. November. https://www.mas.gov.sg/news/speeches/2016/singapore-fintech-journey.
[32] MAS. 2019. Guidelines for E-Payments User Protection. https://www.mas.gov.sg/regulation/guidelines/guidelines-for-e-payments-user-protection.
[33] MAS. 2018. Guidelines on Outsourcing. Singapore. https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing.
[34] MAS. 2019. Payment Services Act 2019. Singapore. https://www.mas.gov.sg/regulation/acts/payment-services-act.
[35] European Central Bank. The Revised Payment Services Directive (PSD2) and the Transition to Stronger Payments Security. https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html.
[36] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
[37] A fintech company, as a payment service provider, is allowed to offer as many as eight kinds of payment services, including issuing of payment instruments, money remittance, account information services, and payment initiation services.

This has enabled fintech companies to tap into bank APIs as payment initiation service providers and account information service providers and offer tailored services to customers, which has resulted in open banking implementation in Europe. The General Data Protection Regulation of May 2018 drives open banking growth by guaranteeing free portability of data within Europe and the customers' rights to decision-making for their own data. It prepares for operational and cybersecurity risks caused by customer data leaks by increasing customers' rights to their own data and the responsibilities of service providers, including personal data processors.

United Kingdom

The United Kingdom (UK) experience shows the importance of revising consumer protection regulations in light of developments in the fintech industry. In response to the growing interest in financial crime risk management, primarily due to the increasing use of customer data by third party service providers, the UK financial authorities are expanding customer data regulations. Specifically, the UK is looking to strengthen customer authentication to prevent financial fraud and enact revised consumer data protection measures. In addition, authorities are enhancing approaches to managing and reporting financial crime risk, such as anti-money laundering, terrorist financing, and fraud. Recognizing more robust regulation related to fintech credit market, the Financial Conduct Authority has been enforcing new rules since December 2019.[38] The regulations include investor protection, which places an investment cap of 10% of investible assets for new or less informed investors, and a minimum scope of disclosure, etc.

POLICY CONSIDERATIONS AND RECOMMENDATIONS

Promote Regulatory Flexibility

Existing regulations centered on traditional financial services should be flexible enough to embrace the latest technology-based financial services to minimize fintech-related risks and ensure improved licensing, regulation, and oversight of fintech service providers. Regulatory arbitrage and a lack of understanding of fintech activity can be addressed by innovation hubs within regulatory agencies and the use of regulatory sandboxes.

Innovation hubs are places where regulators and innovators can interact. By interacting with the fintech industry, regulators can better grasp significant trends as well as potential challenges and hazards associated with novel financial services, as well as the consequences for regulatory policy.[39] Another tool used by regulators is a regulatory sandbox, which allows specific, prequalified firms to soft launch and test their financial services or products under a limited scale or set time frames prior to allowing full approval of a wide scale launch.[40] Given these aspects, the regulatory sandbox can be effective for expanding the use of fintech and incorporating it into the existing regulatory framework. The regulatory sandbox, known as the leading tool for promoting regulatory flexibility, is also expected to provide policy makers and regulators with sufficient time and objective data to prepare for effective fintech policies for financial stability and consumer protection safeguards for new fintech-based financial products and services.

Build Regulatory and Supervisory Capacity

Regulators should be well-equipped with technical capacity to create responsive and unambiguous regulations (footnote 40) and assess sources of information, including untraditional fintech-related data. Further, technology advances at an incredible rate, and regulators should ensure that they stay on top of fintech development in their markets. The rapid growth of technology-driven financial services has increased the need for regulators to create new skills, capability, and an organizational culture that values and encourages innovation.[41] This is also important to better manage risks through innovation hubs and regulatory sandboxes.

The use of new financial technologies to improve regulatory compliance and supervisory oversight are referred to as regtech and suptech tools. While these tools can improve regulation, oversight of fintechs and monitoring fintech-related risks, these tools should be commensurate to the size, complexity, and development of the fintech market and the broader finance sector.[42]

Regtech can facilitate regulatory reporting and address issues such as combating AML/CFT reporting, and suptech generally focuses on misconduct analysis, data management, artificial intelligence analytics, virtual assistance, micro and macro prudential, and market surveillance. Suptech, on the other hand, can be a powerful tool to directly improve supervisory oversight. Under the recent FATF guidelines on the monitoring of Virtual Asset Service Providers,[43] the broader use of new suptech tools is helping regulators better monitor for AML/CFT risks.

---

38 Financial Conduct Authority. 2019. PS 19/14: Loan-Based ('Peer-To-Peer') and Investment-Based Crowdfunding Platforms: Feedback to CP18/20 and Final Rules. London.

39 Asian Development Bank (ADB). 2019. *Asian Economic Integration Report 2019/2020*. Manila. ADB. https://www.adb.org/sites/default/files/publication/536691/aeir-2019-2020.pdf.

40 ADB. 2021. *Asian Economic Integration Report 2021*. Manila: ADB. https://www.adb.org/sites/default/files/publication/674421/asian-economic-integration-report-2021.pdf.

41 Alliance for Financial Inclusion. 2020. Creating Enabling Fintech Ecosystems: The Role of Regulators. https://www.afi-global.org/sites/default/files/publications/2020-01/AFI_FinTech_SR_AW_digital_0.pdf.

42 di Castri et al. 2019. The SupTech Generations. *FSI Insights on Policy Implementation*. No 19. Bank for International Settlements. Basel. https://www.bis.org/fsi/publ/insights19.pdf.

43 FATF. 2021. FATF *Updated Guidance for Risk-Based Approach Virtual Assets and Virtual Asset Service Providers*. Paris.

Strengthen Oversight of Nonbank Payment Service Providers

Nonbank payment service providers have been one of the fastest growing verticals in the fintech space.[44] Given the rapid growth in the digital payments space, tech-enabled criminals have increasingly targeted this sector. To address these concerns and to improve oversight of nonbank payment service providers, national retail payments laws and regulations have been issued and updated in many countries including Japan, Malaysia, the Republic of Korea, Singapore, and Thailand. Regulatory responses often take a risk-based approach to licensing and supervision of nonbank payment service providers. These rules often include a tiered approach to capitalization requirements, the use of trust and escrow accounts to safeguard client funds, cybersecurity standards, tiered know-your-customer rules, enhanced authentication tools, handling alerts, and enhanced internal controls. In relation to payment service providers, regulators should develop a comprehensive approach on financial, operational, and security risks; implement robust initiatives on financial crimes; and build strong industry working groups to ensure better risk management and compliance.

Establish Guidance and Requirements to Mitigate Risks

With the growing role of fintech in financial markets, the gap between fintech regulations and fintech activities is likely to increase potential fintech-related risks. To mitigate these risks, policy makers and regulators should establish timely guidance and regulations to manage financial risks, operational risks, and cybersecurity risks.

Financial risks, especially to interconnected incumbent financial institutions, can be caused by fintech firms operating outside the regulatory framework. To manage potential risks, all fintech firms should go through some form of registration process or licensing depending on the services they offer. Those managing client funds or offering credit or other financial services directly to customers should meet appropriate risk-based and proportionate tiered capitalization requirements. Appropriate reserve requirements for e-money and payment service providers that ensure safeguarding of customer funds should also be in place.[45]

Operational risks are often associated with lack of effective governance, process control, or weak IT infrastructure, which can lead to disruption of financial services. Regulators should set requirements that boards and senior management from fintech firms understand, oversee, and effectively manage—through appropriate process control—any potential risks that might come from emerging technologies. Supervisors should ensure that core risk governance competencies of identifying, measuring, controlling, managing, and measuring risks are in place and that firms have the appropriate resources, skills, and expertise.

Cybersecurity risks in fintech need to be constantly monitored and closely controlled since they can quickly affect financial ecosystems thereby affecting trust and reputation of financial services. Controls should consider the whole ecosystem, especially the roles and connections between fintechs, the broader financial system, and consumers. Regulators can work with industry to provide guidance that is appropriate for their market. These should focus on ensuring that firms have adequate cybersecurity risk management plans in place, requiring certification such as ISO 27001 for information security management.[46]

Update Consumer Protection and Data Protection Regulations

Addressing fintech risks to consumers involves ensuring that financial consumer protection regulations are updated to consider new fintech-related risks to consumers as well as ensuring related data protection practices. These new risks to consumers include updating regulation related to product design and delivery risks, especially in the mobile channel. The regulators should address the potential for overindebtedness specifically for online lending, issues of transparency and unfair marketing practices, consumer complaints and redress, and fraud and cybersecurity.[47] While many policy makers agree on the principle of data privacy and protection in the broader financial system, legal and cultural views vary about how client data can be used, how much disclosure is necessary, and what kinds of controls to give to customers. Among the emerging recommendations, key areas include:

- **Improving data privacy and protection laws** and implementing regulations that adapt these to the digital financial services industry including fintechs.
- **Secure handling and collection of data** utilizing secure protocols (https) while ensuring the transmission and storage of data in encrypted formats. Data should be stored only long enough to satisfy a legitimate business or legal requirement.
- **Informed customer consent,** with clear and simple language about what financial, personal, or transactional data is being collected and how it will be used or shared, with an option to consent or not.
- **Awareness of consequences.** Clients need to know about the data trails and transaction histories they create through digital activity, including the effect it may have credit scores and the right to correct for errors.

[44] Verticals or vertical markets are business niches in which vendors serve a specific audience and their needs; a horizontal market reaches a wide array of individuals regardless of their industry or particular niche.

[45] F. Restoy. 2021. Fintech Regulation: How To Achieve A Level Playing Field. *Financial Stability Institute Occasional Paper.* No 17. BIS. Basel. https://www.bis.org/fsi/fsipapers17.pdf.

[46] ISO/IEC 27001 Information Security Management https://www.iso.org/isoiec-27001-information-security.html.

[47] Center for Financial Inclusion. 2019. *Handbook on Consumer Protection for Inclusive Finance*. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2019/10/Handbook-Consumer-Protection-Inclusive-Finance_FINAL.pdf.

- **Proper internal processes to prevent misuse.**
- **Management and controls for third-party providers** should be the responsibility of the financial services provider. These include lead generators, brokers, agents, and data analytic firms. The regulator ensures that outsourcing agreements cover data privacy, use, and protection.[48]
- The use of **general data ethics principles,** such as fairness, data minimization, transparency, and nondiscrimination, can also be operationalized through algorithmic auditing.

Promote Standardization

National standards for financial technologies can help promote not only interoperability and greater competition but also help manage various risks especially cyber security and risks to consumers. Two areas were standardization in fintech development have helped reduce risks are in the developments around open banking,[49] open finance[50] and QR code payments. Where the support for open banking and/or open finance is being considered, standardization is recommended for safer and more efficient provision of open banking and/or open finance services. In jurisdictions with no standards, fintechs may offer more risky ways to access financial data such as screen scraping. There could also be risks related to the fintech services provided by operators who are not in contractual relationship with banks.[51] Regulators can work with the banking and payment industry to reduce such risks by establishing open banking and/or open finance standards, especially by developing open API standards.[52] Several countries in Asia—Cambodia, India, Indonesia, the Philippines, Singapore, Thailand, Viet Nam, and others have seen the benefits of standardizing QR codes to both reduce the risk of fraud as well as increase interoperability.

Foster National and International Regulatory Coordination

To better address and manage risks for new fintech services, countries will need to ensure appropriate regulatory coordination nationally and internationally. This will not only help avoid regulatory arbitrage, but more importantly, ensure that fintech can develop in a responsible way. Key issues of regulatory coordination include ensuring a level playing field and promoting competition as well as coopetition.[53] This is especially relevant given the entrance of the Big Tech companies that may have a competitive advantage in access to large amounts of client data.[54]

Regulatory coordination and collaboration at the regional and international level, including harmonization of laws and regulations to deal with emerging fintech oversight issues, are becoming increasingly important. It is also important for supervisors to share information as well as experiences, regionally and globally, in order to improve supervisory capabilities. Regional and international coordination can also support the development of international best practices and better address cross-border risks.[55] These include risks associated with cross-border payments, firms that may be offering services not under the purview of the regulator in the receiving or even transacting country, and differences in the way that data privacy is managed in fintechs operating across borders.

---

48 While the following documents were prepared to ensure the development of responsible digital credit, the policies contained here apply equally to fintech providers. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/1970/01/Responsible_Digital_Credit_FINAL_2018.07.18.pdf.

49 BIS. 2019 Report on Open Banking and Application Programming Interfaces (APIs). https://www.bis.org/bcbs/publ/d486.htm.

50 BIS. 2020. BIS Innovation Hub Work on Open Finance. https://www.bis.org/about/bisih/topics/open_finance.htm.

51 Generally, a supervisory body or bank has limited control over a fintech without a contractual relationship. BIS. 2019. The SupTech Generations. *FSI Insights on Policy Implementation.* No 19. Basel. https://www.bis.org/fsi/publ/insights19.pdf.

52 BIS. 2020. Enabling Finance through Open APIs. Basel. https://www.bis.org/publ/othp36.htm.

53 The recent Open Finance regulation in the Philippines was an example of careful consideration of various policy and regulatory issues as well as coordinating with other agencies such as the Philippines National Privacy Commission and close coordination with the industry to ensure coopetition. "Coopetition, a portmanteau of cooperation and competition, is a business strategy where companies simultaneously collaborate and compete with each other". Center for Financial Inclusion. 2018. *Responsible Digital Credit.* https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/1970/01/Responsible_Digital_Credit_FINAL_2018.07.18.pdf.

54 F. Restoy. 2019. Regulating Fintech: What Is Going On, and Where Are The Challenges? Speech at the ASBA-BID-FELABAN XVI Banking Public-Private Sector Regional Policy Dialogue "Challenges and Opportunities In The New Financial Ecosystem". Washington, DC. 16 October. See also Ehrentraud et al. 2020. Policy Responses to Fintech: A Cross-Country Overview. *FSI Insights Policy Implementation.* No. 23. https://www.bis.org/fsi/publ/insights23.pdf.

55 ADB has been supporting exchanges and documenting regional best practices, such as the recently released Fintech Policy Tool Kit for Regulators and Policy Makers in Asia and the Pacific (2022). https://www.adb.org/publications/fintech-policy-tool-kit-regulators-policy-makers. Likewise, efforts such as the Global Financial Innovation Network have continued to share various best practices in fintech regulation and supervision and hold working groups on regulatory and supervisory technologies (regtech/suptech) https://www.thegfin.com.

About the Asian Development Bank
ADB is committed to achieving a prosperous, inclusive, resilient, and sustainable Asia and the Pacific, while sustaining its efforts to eradicate extreme poverty. Established in 1966, it is owned by 68 members—49 from the region. Its main instruments for helping its developing member countries are policy dialogue, loans, equity investments, guarantees, grants, and technical assistance.

ADB Briefs are based on papers or notes prepared by ADB staff and their resource persons. The series is designed to provide concise, nontechnical accounts of policy issues of topical interest, with a view to facilitating informed debate. The Department of Communications administers the series.

www.adb.org/publications/series/adb-briefs

Asian Development Bank
6 ADB Avenue, Mandaluyong City
1550 Metro Manila, Philippines
Tel +63 2 8632 4444
Fax +63 2 8636 2444