REGULATORY CONSIDERATIONS AND SUPERVISORY PRACTICES FOR FINANCIAL TECHNOLOGICAL INNOVATIONS

Regulation for Responsible and Competitive Financial Sector Innovation

June 2020

ASBA

IDB | LAB

This document, *Regulatory Considerations and Supervisory Practices for Financial Technological Innovations*, has been funded by the project ATN/ME-15724-RG (Regulation for Responsible and Competitive Financial Sector Innovation) co-financed by the Association of Supervisors of Banks of the Americas (ASBA) and the IDB Lab, the IDB Group Innovation Laboratory.

For additional information: asba@asbasupervision.org

asbasupervision.com

T. (5255) 5662-0085

Design by Tinta Roja Editoras, contacto@tintarojaeditoras.com

ACKNOWLEDGEMENTS

The Association of Supervisors of Banks of the Americas thanks Juan Pedro Cantera and the other members of the Board of Directors in 2017, for decisively promoting the realization of the project *Regulation for Responsible and Competitive Financial Sector Innovation*. Likewise, and in particular, the Association would like to thank Rudy V. Araujo for his exceptional work and commitment to this project.

This project was possible thanks to the contribution and support of the IDB Lab.

CONTENTS

EXECUTIVE SUMMARY

In recent years, financial markets have experienced deep change due to the introduction of technological innovations. Changes in financial products, services and business models have been profound and will have lasting consequences, as new players test the dominance of incumbent financial institutions. The broad spectrum of new or radically changed ways of providing financial services that we see under the designation of "fintech"[1] has also brought many challenges for financial authorities, not least the need to balance their duty to preserve financial stability with their work promoting greater competition and good customer service in financial markets.

Regulators and supervisors worldwide have reacted, developing novel approaches and tools tailored to their legal and market contexts. Global financial bodies have also been developing a coordinated response to fintech, although such efforts have not yet reached the level of best practices or agreed-upon international standards.

The Association of Banking Supervisors of the Americas (ASBA), recognizing an increasing level of fintech activity in most of its member jurisdictions, decided to embark on a project to assist its members in reaching an informed position regarding relevant fintech-related general topics as well as addressing the challenges brought by specific fintech products. The project's goal is to promote the introduction of these innovative technologies responsibly, sustainably, transparently and competitively.

The document aims to be a useful tool for financial authorities in a rapidly evolving landscape. However, as it takes a regional perspective, and fintech products are introduced in each jurisdiction in a way that reflects local circumstances, the reader should not be surprised to find variations and peculiarities in the local fintech landscape not mentioned here. Moreover, it is imperative for the reader to keep abreast of new fintech developments, both internationally and locally.

Nevertheless, the guidelines presented here should provide an adequate analytical framework for systematically evaluating the most significant topics in the regulation and supervision of fintech, based on principles of risk sensitivity, proportionality, financial stability, transparency and adequate consumer protection, even in those cases where specific fintech products are not yet present.

These guidelines must not be understood as best practices or principles, as fintech is still an evolving area, with new developments continuously hitting the markets. In particular, the convergence of Big Tech[2] and finance is being recognised as a potential game changer by traditional financial institutions and governments worldwide. Therefore, financial regulation and supervisory practices are still changing to adapt to those developments.

Part I presents an analysis of the institutional, legal and technological prerequisites that may impact the efficiency and effectiveness of fintech regulation and supervision approaches. The analysis recognizes the diversity in these three areas among ASBA members and the prerequisites are not intended as barriers to achieving those goals. Rather, identifying the absence of a prerequisite should guide the authority on which of the alternatives offered in the guidelines provide the best options.

Part II of this document contains a set of regulatory guidelines and supervisory practices for fintech products and services. The guidelines neither recommend specific courses of action nor aim to define best practices, but rather offer potential actions that should be evaluated in the context of the legal framework, the financial system structure and the level of fintech development in each member's jurisdiction.

1 "FinTech is defined 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."
Financial Stability Board. Financial Stability Implications from FinTech. June 2017.

2 https://www.bis.org/bcbs/publ/d431.pdf

PART 1

PREREQUISITES FOR THE SOUND IMPLEMENTATION OF TECHNOLOGICAL FINANCIAL INNOVATIONS

INTRODUCTION

The purpose of Part 1 is to identify and describe a set of prerequisites for incorporating fintech products and services into the regulated financial system. Specifically, these prerequisites should promote the adoption of innovative technologies responsibly, sustainably, transparently and competitively. To this end, it is necessary to examine the entry of fintech products from different perspectives.

Chapter II defines those perspectives and other relevant concepts involved in the analysis, such as the role of the financial market structure in promoting or hampering innovation. Chapter III identifies prerequisites linked to information and technological infrastructures, while Chapter IV explores legal requirements. Finally, Chapter V analyses the institutional framework.

It should be noted that lacking one or more of the prerequisites identified in this document does not preclude the successful introduction of fintech products in a specific country. But recognizing those limitations can help a financial authority outline a roadmap to close the gaps.

The analysis identified 16 prerequisites that should help in promoting the introduction of Fintech products responsibly, sustainably, transparently and competitively. The absence of any of these prerequisites in a jurisdiction could be addressed by implementing specific remedial regulations or policies suggested in the guidelines presented in Part 2.

SELECTED DEFINITIONS

Desired characteristics

In order to have a common understanding of the attributes desired while introducing fintech products in the market, it is convenient to delimit what those attributes mean in the context of financial markets and innovations.

Responsibility
Financial responsibility can be broadly defined as the process of managing other people's money and other financial assets in a way that is considered productive and is also in the best interest of the client. This concept encompasses issues related to both market conduct and financial stability.

Sustainability
Financial sustainability is usually understood as the ability of a firm to sell goods or provide services, charging a price that not only covers its expenses, but also creates a profit.[3] Therefore, a financially sustainable financial institution runs its business without requiring external additional funding.[4]

Transparency
Transparency in financial services can be defined as the availability to clients and other outside stakeholders of relevant, reliable information about the characteristics of the products and services, periodic performance, financial position, business model, governance and risks of a financial institution.[5]

Competitive
A competitive financial market is defined as one in which no single financial institution, or group of financial institutions has the power to command prices (interest rates and fees), the supply of products and services, or the entry or exit of other financial institutions. It can require a limit on the share of deposits, loans or assets an individual financial institution has, as well as a degree of homogeneity in products and services among providers.

Market structure and innovation

Market structure (in terms of concentration and contestability) and innovation has long been an issue of debate in economics. Research on the relationship between market concentration and innovation *"has produced conflicting findings"*.[6] Earlier research specific to financial market structure and innovation seems to suggest that market concentration facilitates innovation. An analysis of the adoption of automatic teller machines (ATMs) found that *"larger banks and banks operating in more concentrated local banking markets register a higher conditional probability*

3 This definition is compatible with unprofitability in the first few years of a start-up or aggressive pricing (below costs) in some products or services in order to gain market share.
4 Another view of sustainability looks at the financial institution's activities' impact on the environment. This perspective goes beyond the scope of the project.
5 Adapted from bushman, R.M. Transparency, Accounting Discretion, and Bank Stability. In: FRBNY Economic Policy Review August 2016. Page 129.
6 UGUR, M. and Hashem, N. Market Concentration, Corporate Governance and Innovation. In: Journal of Governance and Regulation / Volume 1, Issue 3, pp. 199-215. 2012.

of adopting this new technology".[7] Frequently, oligopolistic banks developed proprietary ATM and point of service (POS) networks, creating a barrier to entry for smaller banks that could not afford to build such networks. The inefficiency of this setup was borne by customers.

Thus, the question is:

> Does concentration have an effect on how a technological innovation alters management's incentives at incumbent financial institutions?

The answer to this question exceeds the scope of this document. Nevertheless, is important to keep in mind that it is possible that the degree of financial market competitiveness affects innovation, and vice versa.

How fintech products enter the market

One of the main challenges for regulators when deciding how to approach the introduction of innovative products or services into the market nowadays is the wide diversity of ways this could take place. While previously the innovation route usually started and remained within established financial institutions, with fintech an innovation could take a more convoluted path, each demanding specific prerequisites. For the purpose of this analysis, four modalities will be considered:

By a newly created firm (start-up)
This is the route most commonly associated with fintech. Although these firms are usually outside the regulated financial system, their products could be indistinguishable from those offered by regulated financial institutions. Also, these firms can become regulated, sell their innovative product to a financial institution or acquired by a regulated firm.[8]

By a regulated financial institution
This is the traditional route. It should be noted that under this mode, the innovation can be introduced without prior knowledge by the regulator, especially when it involves an internal process or business model already adopted by a parent company in another country.

By an existing non-financial company
In this case, a technological, telecommunications or other type of non-financial company introduces a fintech product, leveraging its existing customer base to rapidly achieve critical mass. That distinguishes this mode from the start-up model.

By a non-resident firm, remotely
Many fintech products, by their nature, do not require a provider's physical presence to enter a market. This allows these firms to compete, in effect, in the same market with regulated financial institutions. This modality includes the three aforementioned, but provided remotely.

Let's turn now to the areas and the corresponding prerequisites.

7 Hannan, T.H. and Mcdowell, J.M. 1984. The determinants of technology adoption: the case of the banking firm. In: Rand Journal of Economics. Vol. 15, No 3. Autumn 1984.

8 Basel Committee on Banking Supervision. Core Principles for Effective Banking Supervision. 2012. Principle 7: "Major acquisitions: need prior supervisory approval as per prescribed criteria to ensure that any new acquisitions or investments do not expose the entity to undue risks or hinder effective supervision."

INFORMATION AND TECHNOLOGICAL INFRASTRUCTURE

By definition, this is the most relevant area to consider. Most, if not all, fintech products need the availability of certain basic communications and related services satisfying specific levels of quality and reliability. Also, those working in fintech development and provision must satisfy particular professional skills.

It should be noted that most policy documents analysing fintech take for granted that the required physical and communicational infrastructure is already in place, which is not necessarily the case in every country in a region. This is clearly revealed in the assessments done by the International Telecommunication Union, the specialized United Nations agency responsible for issues that concern information and communication technologies. Its ICT Development Index ranks 176 countries based on their level of ICT use, access and related technical skills. Although some ASBA members score high in the index, other countries rank well below the worldwide midpoint.[9] Therefore, it is important to assess the suitability of the ICT infrastructure.

This chapter presents the prerequisites, from the most obvious and basic to the more specific.

Reliable telecommunications networks

In essence, financial services and products involve data processing and transmission. Fintech products are no exception. Moreover, fintech developments have accelerated the prevailing trend in finance away from physical based records and on-site processing to a more distributed model. Fintech products usually require that customers, as well as areas within a financial institution, send information to a remote site, through a variety of digital channels, in order to carry out transactions.

As the International Monetary Fund (IMF) and the World Bank expressed: *"the infrastructures should enable efficient data collection, processing, and transmission, which are central in Fintech advances."*[10]

A non-reliable data network exposes customers and service providers to disruptions that can easily translate into financial losses. Traditional financial systems have operated for decades on trusted closed data networks, such as SWIFT at the international level and similar robust and redundant communications infrastructure, usually operating under a restricted membership scheme.

Fintech developments have led to a more eclectic approach, with promises of cheaper and quicker data transmission using open communication channels, based on the internet. However, open TCP/IP networks, by design, are not as robust as closed data networks.

Therefore, unless the communications infrastructure[11] is robust enough, the implementation of fintech products cannot be deemed responsible, in particular when it occurs outside traditional financial institutions.

9 International Telecommunication Union. Measuring the Information Society Report. Volume 1. 2018.

10 International Monetary Fund and the World Bank. The Bali Fintech Agenda. October 2018.

11 Basel Committee on Banking Supervision. Core Principles for Effective Banking Supervision. 2012, Principle 26.

Wide access to networks and suitable devices

In order to fulfil the expected benefits of fintech in terms of fostering greater competition in the financial market, associated products and services should be widely available, both in terms of geographic coverage and choice of communication channels.

For this reason, the IMF encourages authorities to *"facilitate the development of telecommunications, broadband, and mobile data services—including in rural areas—and the achievement of sustainable universal access. Attention should be paid to ensuring a basic quality of service and affordability across customer segments."*[12]

A related issue is the availability and affordability of devices suitable for financial services. Some fintech products launched in developing economies have been forced to compromise on security features, as most customers' devices lack enough processing power or use old data transmission protocols.

A clear example of this compromise is one of the earliest fintech products, M-Pesa, a mobile wallet developed by Safaricom, a Kenyan telecom company. The service relies on SMS (Short Message System) for all its data interchange between the company and its users. However, it is widely known that *"the security afforded by SMS is not sufficient for financial transactions."*[13] Nevertheless, in countries where the population cannot afford to own modern devices that are able to access more secure channels, the introduction of fintech products could prove unsustainable, as the potential customer base is probably small.

Adequate level of technically skilled professionals

Firms offering fintech products require a minimum of suitably skilled staff, even if the firms acquire products from other companies. Routine maintenance, troubleshooting, security monitoring and adaptation to the local environment are tasks normally performed by their own permanent staff. Bringing in fintech products from other markets without having the required skilled staff on hand cannot be described as responsible.

Furthermore, it would be appropriate that these professionals are required to comply with transparent technical and ethical standards set and enforced by official or professional bodies consistent with international standards.

It should be recognised that there are shortages of skilled IT staff even in advanced economies. This is more evident for staff with combined IT and finance skills. A report by a fintech industry body in the United Kingdom stressed that there is a *"global shortage of talent in the Fintech sector."*[14] According to International Telecommunications Union's (ITU) ICT Development Index, economies in Latin America and the Caribbean, on average, have a higher level of ICT skills, although with huge disparities among countries.

Effective interoperability in telecommunication and payment systems

Interoperability between data networks as well as between payment systems is a crucial prerequisite to ensure all four desired attributes are achieved when introducing fintech products. This concept goes beyond the basic technical layers of interoperability, syntactic and semantic interoperability, when two or more systems are capable of communicating with each other and are able to automatically interpret the information exchanged, respectively.

This information exchange must be subject to clear and known economic terms, such as fees and limits. Without interoperability, the introduction of fintech products could potentially result in a non-competitive outcome, such as mandatory contracts with a specific mobile network operator (MNO) to use a mobile wallet. Also, for an independent provider of a fintech product, having to negotiate access

12 Idem.

13 Nyamtiga, Sam and Laizer. Security Perspectives For USSD Versus SMS In Conducting Mobile Transactions: A Case Study Of Tanzania. In: International Journal of Technology Enhancements and Emerging Engineering Research, Vol 1, Issue 3. 2013.

14 Innovate Finance. Supporting UK Fintech: Accessing a Global Talent Pool. April 2018.

to data networks individually with several companies could affect its sustainability.

Furthermore, the accumulation of exchange fees paid by the fintech provider probably will affect price transparency for its users.

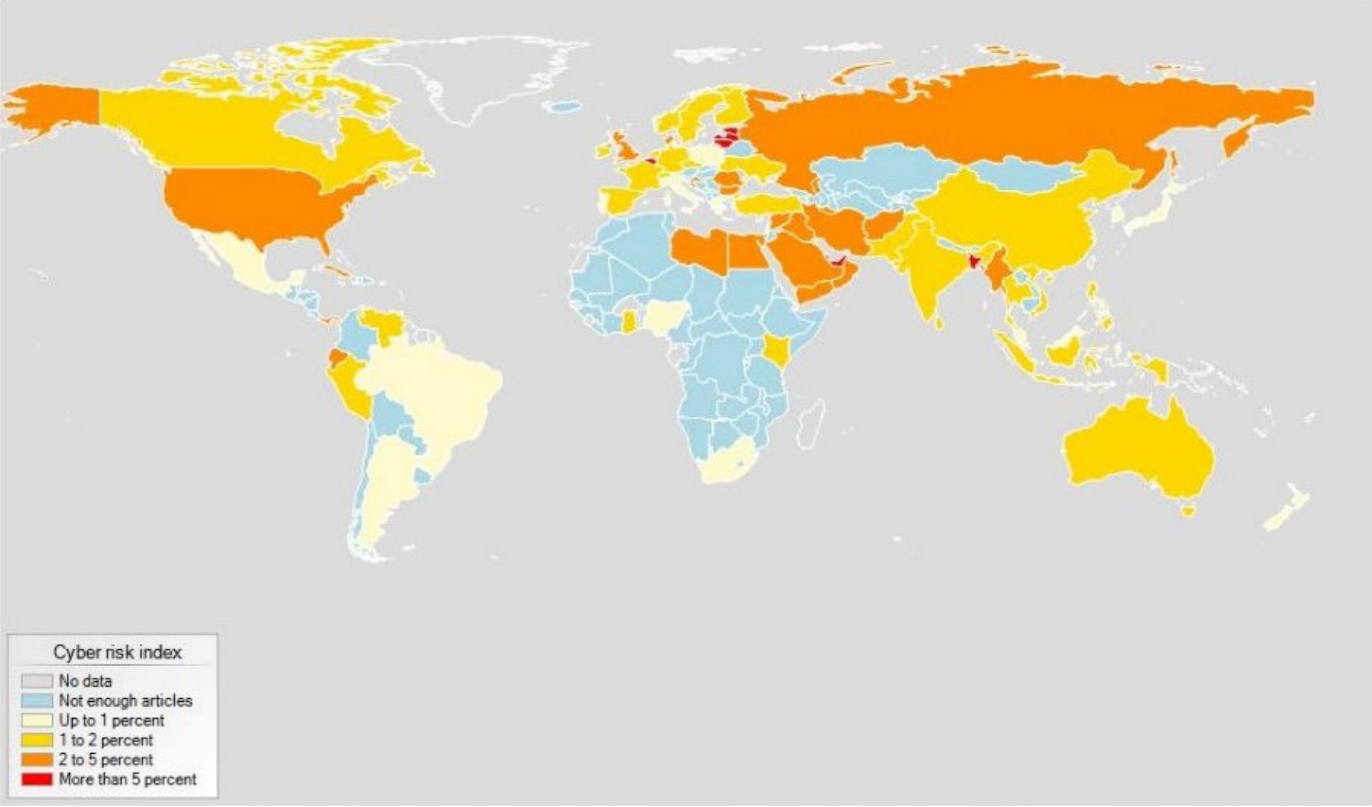
A clear example of this scenario is, again, M-Pesa. Safaricom initially restricted access to the mobile wallet only to its telephony subscribers. This resulted in a quasi-monopolistic stronghold in mobile money in Kenya and prices that were substantially higher than those charged by other MNOs that started to offer similar products later. After several years of enjoying this dominance, in 2014 Kenya's competition authority ordered Safaricom to allow other competitors to use its network and not to levy extra charges on money transfers to or from customers of other MNOs.[15]

There is a national Computer Emergency Response Team

As financial services have increasingly become digital processes, with fintech the purest example, there has been an

15 Competition Authority of Kenya. CAK Orders Safaricom to Open up M-Pesa. July 2014.

Figure 1: Measure of cyber risk of banks



Note: Number or articles featring "cyber-attack" or "hack" or "cyber risk" or "cyber security" and "banks" or "bank" and "risk" divided by the number of articles featuring "banks" or "bank" and "risk" by country. The index is not computed for countries with fewer thar 25 articles on cyber risk (light blue). Only articles in English were included. Period range: Jan. 2014-Sep. 2017.
Sources: Factiva; and author's calculations.

increase in cybersecurity events. The impact of these events, *"in a world where everything from room heaters to wearable fitness trackers is connected,"*[16] has increased in frequency and monetary value. In parallel, the speed at which stolen funds or private financial data has been transferred to other jurisdictions has also accelerated. The cybercrime global scale can be better seen in Figure 1, showing the national 'Cyber risk index' for banks, created by the IMF and based on the frequency of keywords in press articles.[17]

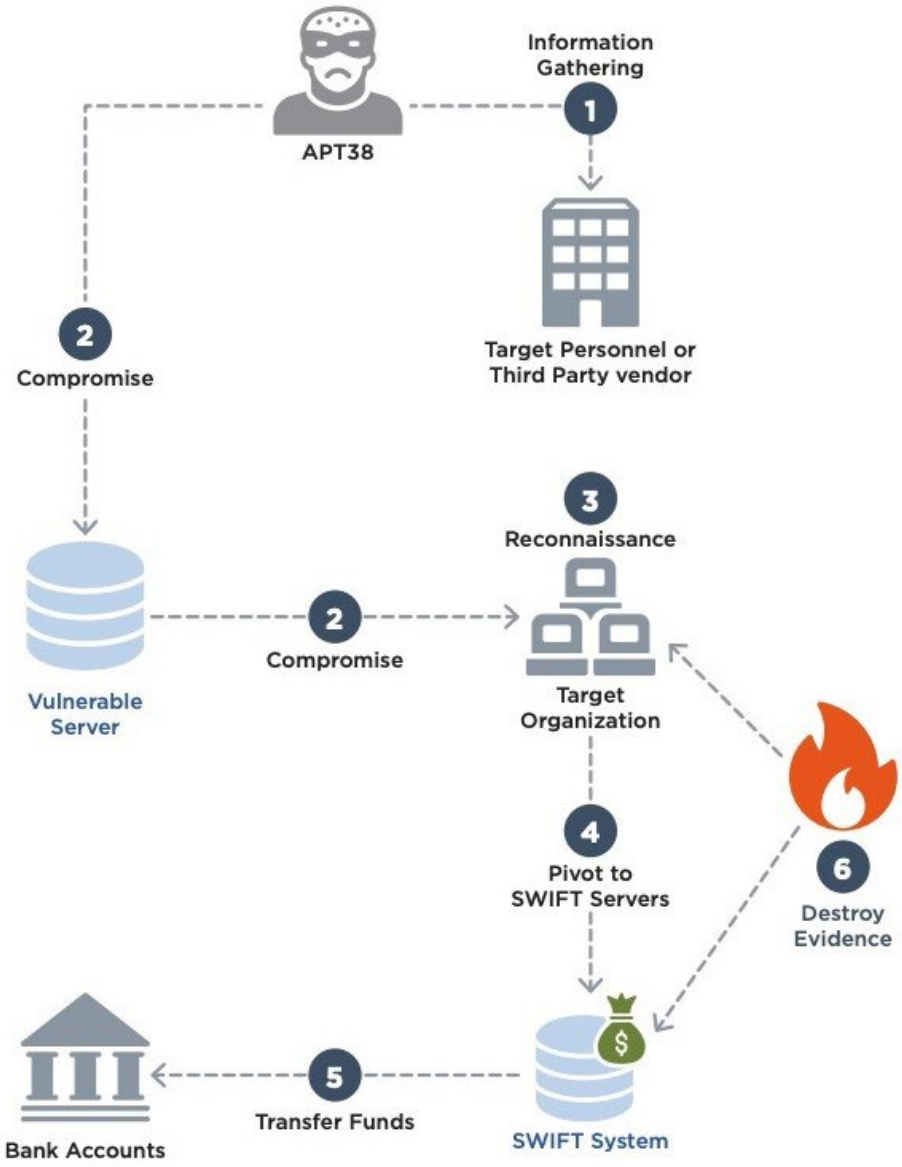
The same report compiled attacks on fintech firms, resulting *"in at least USD 1,450 Million in losses due to fraud since 2013."*[18] Such incidents rarely occur in isolation. Rather, the norm is that cyberattacks are carried out using several unwitting parties, such as telecommunications companies, cloud service providers and other third parties. Also, the involvement of state-sponsored hackers cannot be ruled out. Figure 2 describes how a suspected North Korean group attacked several firms, including two large banks in Latin America.[19]

Therefore, in some countries it is evident that the financial sector, including fintech firms, which are especially vulnerable, requires a single point of contact to get assistance when subject to cyberattack. The United Nations has proposed the *"creation of public-private partnerships between regulators, DFS providers, and banks to monitor cyber threats as they arise. These may include: Computer Emergency Response Teams. These have been established in a number of countries at national and regional levels to quickly collate, identify, and coordinate responses to cyber-attacks"*[20] as a key element of a resilient financial market, conducive to financial inclusion.[21]

According to the International Telecommunications Union (ITU), as of March 2019 there are currently 109 national Computer Incident Response Teams (CIRTs) worldwide. To date, ITU has established or enhanced CIRTs in 14 countries and completed CIRT Assessments for 75 countries. In addition to coordinating cyber-related incident responses, other CIRT responsibilities may include: distribution of advisories and alerts, continuous monitoring, risk assessments and research and development.

16 Padmanabhan, A. Designing Cybersecurity for the Financial Sector. In Livemint. May 2017.
17 Bouveret, A. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. IMF Working Paper WP/18/143. 2018.
18 Idem.
19 FirEye. APT38 Un-usual Suspects. October 2018.
20 United Nations Secretary-General's Special Advocate for Inclusive Finance for Development. Briefing on Cybersecurity. 2018.
21 A National Financial Inclusion Strategy may be complementary to a National Cyber Security Strategy.

Figure 2: An APT38 cyber bank robberty



LEGAL FRAMEWORK

The disruptive nature of fintech means that, in many aspects, the prevailing legal framework is not adequate to address some of the challenges it poses on regulators. This chapter examines the elements in legislation that are conducive to a successful introduction of fintech products.

It should be emphasised that the purpose of this section is not to suggest changes to the current legal framework in ASBA members' countries. Rather, any perceived gap between these prerequisites and the set of laws and rules should be taken into account when setting a policy approach towards fintech.

Some of the following prerequisites match elements of the Basel Committee on Banking Supervision's (BCBS) Core Principles for Effective Banking Supervision (CPEBS).[22] In those cases, a reference to the corresponding principle is made.

The supervisor can take pre-emptive action regarding unlicensed restricted financial service provision

The law should grant the financial supervisor powers to take action when it identifies the provision of restricted financial services by non-licensed firms. According to the specific legal framework, it could be possible for the supervisor to decide whether or not to exercise this power, in line with its policy approach.

It is to be expected that this legal power will reduce the likelihood of harmful unlicensed fintech activities and encourage potential fintech firms to contact the supervisor before engaging in financial activities.

The range of financial services subject to control should be in line with CPEBS Principle 4 - Permissible activities.

The law grants the authority the power to designate a product/service as financial intermediation

Some fintech products are not easily categorized as financial intermediation products or services.[23] The standard model of clear demarcation between a bank that accepts deposits, grants loans and takes on credit, liquidity and pricing risks and an investment brokerage house that takes none, does not always apply in the fintech world.

Firms offering services such as peer-to-peer (P2P) lending and crowdsourcing could claim that they merely provide a meeting place for customers willing to lend and borrow money. If customers themselves select all the relevant elements of a transaction - counterparty, amount, currency, maturity, interest and repayment schedule – it is not self-evident that the fintech firm is engaging in financial intermediation.

Therefore, the authority will need to carefully analyse the fintech product and, if it judges that the product

22 Basel Committee on Banking Supervision. Core Principles for Effective Banking Supervision. 2012.

23 Organisation for Economic Co-operation and Development. Glossary of Statistical Terms.

shows all or some key elements of financial intermediation, the supervisor must have the power to treat the product as such.

The law allows the authority to apply the same rules to cross-border provision of financial services and domestic-based services

Technology is enabling firms to provide financial services remotely, without a physical presence in a country. Using existing links between local payment systems and external financial institutions, a customer can engage in financial activities outside the scope of local authorities.

Whereas in the past, cross-border transactions for individuals were usually restricted to high-net-worth customers through specialized wealth management firms, the easing of foreign exchange restrictions and new communications platforms have expanded access to cross-border transactions to almost every customer. Fintech firms and their associated products are usually present in this trend."[24] *A wave of neo-banks such as Revolut have well and truly captured the attention of consumers globally, with digital-only offerings that support the cross-border needs of global citizens.*"

In parallel, firms offering remote access to financial services are not necessarily subject to regulation and/or supervision in their countries of origin. Thus, the decades-old effort by authorities to set a cooperation framework to deal with cross-border activities by financial institutions, started by the 1975 Basel Concordat, is showing its limitations, mostly as a result of technological innovations. For the Financial Stability Board, *"innovations in cross-border lending, trading and payment transactions, including via smart contracts, raise questions about the cross-jurisdictional compatibility of national legal frameworks."*[25]

Although it appears there is yet no satisfactory legal approach to this issue, in order to avoid undesired outcomes from the implementation of fintech products, **the legal framework should include provisions allowing authorities to extend the scope of local regulations to services and products provided by firms located abroad.**

This prerequisite should be consistent with CPEBS Principle 13 – Homes-host relationship.

The law defines and punishes cybercrime

The shift to a society where many interactions take place in electronic form has inevitably meant that criminal activities, specifically of the financial sort, but also of the relevant authorities, are now focused on transactions taking place in the virtual realm. Many of these offences were not clearly defined in pre-21st Century criminal codes. Most countries have already changed their laws to cover cybercrimes, but not all have. The United Nations Conference on Trade and Development indicates that *"138 countries (of which 95 are developing and transition economies) had enacted such legislation. However, more than 30 countries had no cybercrime legislation in place."*[26] In a survey of ASBA members' legal counsels made in Component I of this Project, 6 out of 23 members indicated their legal frameworks do not define cybercrime.

Definitions vary from country to country but usually include two sets of activities: *"Cyber-dependent crimes - crimes that can be committed only through the use of Information and Communications Technology devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity) and Cyber-enabled crimes - traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft)."*[27]

24 Houseman, D. KPMG: 2018 Was the Year of Democratization. December 2018.
25 Financial Stability Board. Financial Stability Implications from Fintech. June 2017.
26 UNCTAD. Cybercrime Legislation Worldwide. Accessed on March 2019.
27 The Crown Prosecution Service (United Kingdom). Cybercrime-prosecution Guidance. Accessed March 2019.

However, it should be noted that most legislative actions have a narrow focus on specific issues, leading to *"a growing legal fragmentation at international and national level."*[28] **This evolution poses challenges when dealing with criminal activities in the financial sector, as activities outlawed in a country may be not punishable in the country of origin of the perpetrator**. This absence of dual criminality is somehow addressed in the FATF recommendation 37 and allows for the country to render mutual legal assistance, if the assistance does not involve coercive actions and encourages countries to consider adoption of such measures as may be necessary to enable them to provide a wide scope of assistance in the absence of dual criminality.

The recommendation further advises that where dual criminality is required for mutual legal assistance, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

The issue arises of whether a financial authority should take into account this legal asymmetry when analysing cross-border provision of fintech products.

Nevertheless, in order to foster a responsible and sustainable fintech ecosystem, the legal framework must protect consumers, providers and other stakeholders against criminal activities, in concordance with CPEBS Principle 29 - Abuse of financial services.

The law makes it mandatory for all firms to disclose cybersecurity events

For both users of fintech products and firms providing them, it is important that every company in the product or service supply chain discloses, promptly and fully, any material incident involving malicious access to systems and data. By design, in most fintech products multiple companies each play a crucial role handling customer data and instructions in the supply chain, such as telecommunications companies, cloud data storage and processing providers and other ancillary services.

Also, **for supervisors and regulators it is important to gain early knowledge of such events, as in some cases these could potentially have systemic consequences**. As a recent study by the IMF indicated, *"Cyber risk has emerged as a systemic risk concern, following recent cyber incidents."*[29] Standing out among such events are the attempted heist of USD 1 billion from the Bangladesh Central Bank in 2016 and a virus attack on three major South Korean banks in 2013, which froze their computer systems and left many South Koreans unable to withdraw money from ATMs. A similar attack in 2018 affected some Mexican banks' connection to the interbank money transfer system run by the central bank, SPEI. Although the amount stolen was low (US$ 15 million), it slowed down this key service.

Without this information, providers of fintech products relying on long supply chains will find it difficult to properly and promptly assess cyber risk. As the IMF document expresses, *"data on cyber incidents is scarce and there have been very few quantitative analyses of cyber risk. Data on cyber risk is notoriously scarce, since there is no common standard to record them, and firms have no incentives to report them. [Moreover,] "international sharing of data reported to domestic regulators also has to take into account - beyond the typical privacy and other constraints - that there might be national security considerations in sharing and reporting of data."*[30]

In order to promote a sustainable, responsible and transparent environment for fintech products, it is clear that there should be an explicit requirement for all companies to disclose, in a standard format, any cybersecurity events, at least to the authorities and the fintech firms reliant on the affected services, in accordance to BCBS Principle 25: Operational risk and Principle 28: Disclosure and Transparency.

28 United Nations Office on Drugs and Crimes. Comprehensive Study on Cybercrime. 2013.

29 Bouveret (2018).

30 Idem.

Furthermore, as per BCBS Principle 10: Supervisory reporting, there ought to be means of enforcing compliance with the requirement that information be submitted on a timely and accurate basis. The appropriate level of the entity's senior management where the responsibility lies must be determined. Thus, pending issues require authorities to think about who must prescribe the standardised format for disclosing cybersecurity events and what is an acceptable timeframe for disclosure.

The law should endorse data privacy rights

Fintech has made it clear that, at its core, financial services use customer data as their raw material. The features long associated with banking, such as branch networks, physical interaction and paper handling, are rapidly losing their relevance in modern finance. Customer data in general, not just on their financial transactions, is now available in digital formats and is being used to analyse and generate insights on spending patterns and other behavioural traits.

A report by the World Economic Forum focused on the appropriate use of customer data in financial services describes the current situation in the following words:

> *"Whether it is data breaches at large organizations crucial to the provision of credit, disclosures of controversial data-sharing practices at social media firms offering payment services, or considerations by big techs to partner with banks and exchange customer and transaction data, the accelerating data-fuelled transformation of financial services demonstrates the need for stakeholders to align on principles governing the use of customer data. Uncertainty about what it means to use customer data appropriately could cause a loss of trust that could lead to instability in the financial services system."*[31]

In order to ensure that fintech products make appropriate and responsible use of customer data, the law should establish clear safeguards that balance customer data oversight and innovation, as well as allow for appropriate recourse when warranted. These safeguards should apply to every type of company handling personal data and involve *"attain[ing] customer agreement to their customer data policies and, where appropriate, seek[ing] consent for specific uses... [and also] customers should be able to request that data about them no longer be used by an organization..."*[32]

It should be noted that the right to data privacy and protection could be used by incumbent financial institutions to set anticompetitive barriers, effectively blocking new fintech product providers from engaging with customers.

It must be recognized that while data privacy laws are being enacted in most countries, few countries are considering the anticompetitive effects of such laws, mostly outside finance. The European Union (EU), through the Payment Services 2 Directive,[33] in force since mid-2018, has articulated a response to those effects, by mandating financial institutions and other regulated participants in the EU payment system to allow access to each other's customer data, if the customer explicitly gives consent, a policy commonly known as 'Open Banking.' This is a form of the right to 'data portability' enshrined in EU legislation.[34] This policy relies on the technology 'application programming interface' (API) which is essential for several fintech products and essential for several fintech products.

In parallel, the United Kingdom's authorities are working with the industry to manage an orderly introduction of this policy, through the Open Banking Implementation Entity, a company set up by the Competition and Markets Authority.[35]

31 World Economic Forum. The Appropriate Use of Customer Data in Financial Services. September 2018.

32 Idem.

33 EU. Payment services (PSD 2) - Directive (EU) 2015/2366.

34 EU's General Data Protection Regulation introduced the right for data subjects to receive the personal data that they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without hindrance.

35 See Open Banking.

Mexico also passed a fintech-focused law[36] setting the legal footing for the mandatory implementation of open banking system-wide, within a timeframe of 24 months.

However, it must be recognized that these are still very recent developments and, thus, open banking remains an unproven concept. Other authorities have preferred non-mandatory routes *"to promote and accelerate the take-up of data sharing frameworks in banking."*[37] Therefore, at this time it is not possible to categorize open banking as a prerequisite.

The law gives the supervisor the power to require regulated financial institutions to provide advanced knowledge of new services, products, processes or business models

This pre-requisite comes in accordance with CPEBS Principle 10: Supervisory Reporting, i.e. the supervisor is to have the power to require fintech firms to submit information on financial conditions, performance and risks, internal management and matters deemed relevant, on demand and at regular intervals.

In early 2018, the BCBS sketched five forward-looking scenarios to assess the impact of the evolution of fintech products on the banking industry:[38]

a) The better bank: modernisation and digitisation of incumbent players.
b) The new bank: replacement of incumbents by challenger banks.
c) The distributed bank: fragmentation of financial services among specialised fintech firms and incumbent banks.
d) The relegated bank: incumbent banks become commoditised service providers and customer relationships are owned by new intermediaries.
e) The disintermediated bank: banks become irrelevant as customers interact directly with individual financial service providers.

Although it is difficult to determine, based on current information, which scenario will prevail, it is possible to assert, based on the structure of financial markets, that in most Latin American and Caribbean countries the most likely scenario is the revamping of incumbent banks. Although in some countries[39] there is a lively fintech ecosystem with many new start-ups, most remain fairly small and so far, unable to approach the size of traditional banks. Many of those start-ups have identified the unbanked as their most likely target, a significant proportion of the economically active population and one markedly underserved by traditional banks.

Another fact to take into account is the sizeable proportion of financial institutions in the region with headquarters in developed economies. Almost all of these financial institutions are actively engaging in introducing technological innovation, either by in-house development, or by acquiring products or fintech start-ups in their home countries and other developed markets. Reinforcing this trend is the expectations of most fintech start-ups in those markets, where *"75.5% of Fintech surveyed want to collaborate with traditional financial services firms. Only 18.1% want to compete on their own. The rest want to be acquired by other Fintech or traditional firms."*[40]

This brings to the fore the question on how large and systemically important banks in the region's markets will implement innovations. **It can be safely assumed that for most international financial institutions, technological innovation, especially in internal processes, will be an instruction from the head office.**

For the supervisor, interested in ensuring that such innovations are implemented responsibly and transparently,

36 Mexico. Ley para Regular las Instituciones de Tecnología Financiera. March 2018 (In Spanish).
37 Deloitte. Open Banking Around the World: Towards a Cross-industry Data Sharing Ecosystem. November 2018.
38 Basel Committee on Banking Supervision. Implications of Fintech Developments for Banks and Bank Supervisors. February 2018.
39 Five countries, Mexico, Brazil, Argentina, Colombia and Chile, account for 86% of the fintech companies in the region, according to a report by the Inter-American Development Bank: Fintech Latin America 2018. November 2018.
40 Capgemini. World Fintech Report. 2018.

it is important to be aware of the changes, to understand the fintech product and to ascertain that the financial institution has followed the appropriate risk management activities while evaluating the new products in the country, in line with BCSB Principle 15: Risk management process.

The country has enacted antitrust legislation that applies to the financial market

Fintech has been widely proclaimed as an effective tool for promoting competition in financial markets. However, this is not an inevitable outcome. In fact, the actual implementation of fintech could well result in a less competitive financial market. The M-Pesa experience, described before, is a helpful reminder that technological innovation does not preclude market dominance by one or a few firms.

Previously interoperability, effective access and data portability were identified as key elements in ensuring a competitive outcome from the implementation of fintech. However, a study commissioned by the European Parliament, while recognizing the pro-competition potential of fintech, says that *"some factors can result in anticompetitive behaviours, namely the network effects derived from the use of online platforms, the access to customer data, standardisation, interoperability and the use of algorithms."*[41]

In particular, the study highlights how current concerns regarding the market power of large technological firms such as Google and Facebook in areas such as cloud computing and data handling can extend to financial markets as those firms become players in these markets.

In a similar vein, Netherland's Authority for Consumer and Markets considers that *"Fintech may be an important driving force for competition, consumer choice and innovation in the market. However, it may also bring new risks for competition."*[42]

This seeming contradiction was expressed as a still unanswered question by Agustin Carstens, General Manager of the Bank for International Settlements: *"Will big tech's involvement in finance lead to a more diverse and competitive financial system or to new forms of concentration, market power and systemic importance?"*[43]

The EU Parliament study concludes by indicating that *"the current level of competition in the Fintech ecosystem does not suggest the need for any urgent change regarding the competition policy tools,"*[44] while recognizing that some European competition authorities, such as the German Commission on Monopolies, have proposed changes to competition legal tools.

This awareness of the potential threats to competition in the financial markets from fintech emphasizes the need for authorities to have at least basic anti-trust legislation in order to avoid uncompetitive outcomes from the introduction of fintech products.

The country has a general consumer protection framework

The potential risks and challenges arising from the introduction of fintech products and the need for an appropriate consumer protection framework have been extensively analysed in the previous components. This requirement predates fintech, and there is an international consensus that *"financial consumer protection should be an integral part of the legal, regulatory and supervisory framework, and should reflect the diversity of national circumstances and d global market and regulatory developments within the financial sector."*[45]

The arrival of technology-driven financial services has raised the need for this framework, as "digital financial services also

41 European Parliament. Competition Issues in the Area of Financial Technology (Fintech). July 2018.
42 De Autoriteit Consument & Markt. Fintech and Competition. June 2016.
43 Carsten, A. Big Tech in Finance and New Challenges for Public Policy. December 2018.
44 Idem.
45 G20 Finance Ministers and Central Bank Governors. G20 High-Level Principles on Financial Consumer Protection. October 2011.

carry new risks for financial consumers."[46] Some of those new risks arise from the use of non-traditional distribution channels and non-regulated firms to provide consumers with financial services. "*This can encompass uneven levels of protection within (e.g. inadequate disclosure and redress mechanisms) and across countries (e.g. variety of providers, cross border selling, regulatory arbitrage); consideration of data protection issues; a lack of coordination among authorities for example with respect to new types of digital financial services.*"[47]

In order to mitigate the negative consequences of delayed or non-existent redress actions by the authorities in cases where the consumer is mistreated by an unregulated provider, a general consumer protection regime can ensure a minimum level of protection even in cases where the financial authority cannot take direct action.

46 G20/OECD Policy Guidance Financial Consumer Protection Approaches in the Digital Age. 2018.

47 Idem.

INSTITUTIONAL FRAMEWORK

This chapter explores which institutional arrangements are conducive to having the introduction of fintech result in the desired outcomes outlined in Chapter II. The emphasis is on identifying inter-institutional links that require the acquiescence of institutions other that the financial regulator and/or supervisor.

There should be effective and robust cooperation arrangements among domestic authorities

Fintech activities have implications across many areas of public policy: finance, telecommunications, competition, Anti-Money Laundering/Combating the Financing of Terrorism (AML/CTF), national security, to name the most relevant. In some countries it is even seen as part of the national economic development strategy. Therefore, it is not uncommon to see multiple authorities involved in decisions affecting fintech developments, sometimes with conflicting stances.

In this sense, authorities must be aware that CPEBS Principle 1: Responsibilities, objectives and powers, certainly defines a set of actions that must be established. *"Clear responsibilities and objectives are to be assigned for each authority involved in the supervision, clearly defined in legislation and publicly disclosed. Where more than one authority is responsible for supervision, a credible and publicly available framework is in place to avoid regulatory and supervisory gaps."*

Given the multiple paths that fintech products can use to enter into a financial market, as indicated previously, a lack of communication among domestic authorities could well end up in undesirable outcomes, either impeding the development of beneficial services or letting regulated activities be performed by unregulated firms. In the latter case, the likely negative consequences should be minor and circumscribed to market misconduct.

However, in some instances a lack of coordination among authorities has created a policy vacuum that is harming a sustainable and competitive fintech ecosystem. A report by the US Government Accountability Office found that *"with numerous regulators, Fintech firms noted that identifying the applicable laws and how their activities will be regulated can be difficult. Although regulators have issued some guidance, Fintech payment and lending firms say complying with fragmented state requirements is costly and time-consuming."*[48]

On the other extreme, the crash of the P2P industry in China shows how market misconduct carried out at a massive scale could risk becoming a systemic problem for authorities. *"The P2P lending industry in China has emerged and thrived in a regulatory vacuum. For a long time, it was unclear who is a responsible regulator for the market; and there were only rare and piecemeal rules governing the P2P lending activities. These rules spread across Criminal Law, Consumer Law, Securities Law, and judicial interpretations of the Supreme People's Court."*[49]

Under the then-prevailing wait-and-see policy approach towards fintech and P2P in particular, the four relevant

48 US Government Accountability Office. Financial Technology Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight. March 2018.

49 You, Ch. Recent Development of Fintech Regulation in China: A Focus on the New Regulatory Regime for the P2P Lending (Loan-based Crowdfunding) Market. In: Capital Markets Law Journal, Volume 13, Issue 1. January 2018.

agencies - central bank, securities, insurance and banking regulators – basically just watched as thousands of firms sprung up to engage in this activity since the first was founded in 2006.

In monetary terms, the sums involved (about US$ 200 billion at its peak) were significant although small within the wider Chinese context. Nevertheless, as the traditional banking system was confronting problems with originating loans to its traditional clientele of State-owed large corporations, P2P platforms rapidly gained space, lending to SMEs. *"The ratio of new P2P loans to new bank loans rose to almost 40% in June 2016."*[50]

In this unregulated landscape, inevitably many of the new firms were engaging in risky practices or outright fraud: *"By the end of 2015, there were 1,031 total troubled platforms out of 3,448 platforms still in operation. So, on average, one out of four was problematic."*[51] *"Risks rose due to inappropriate market practices and fraud, including Ponzi schemes."*[52] When the number of clients affected rose steeply, the authorities reacted in 2016 by issuing a single body of regulations, and a large number of P2P firms collapsed, unable to comply with the new regulations. It is projected that by the end of 2020, just a few dozen P2P firms will remain in the market.

Both examples illustrate the relevance of clear coordination among relevant authorities to ensure that the expected benefits of fintech effectively crystallize, in line with CPEBS Principle 3: Cooperation and collaboration and Principle 8: Supervisory Approach.

There are flexible and working cooperation agreements with overseas regulators

Just as important as coordination among domestic authorities, a sound regulatory approach to fintech requires that the financial authority can effectively ask for and obtain help in dealing with fintech product providers operating outside its jurisdiction. The last few years have seen a surge of memorandums of understanding between financial authorities specifically touching on fintech.

"Fintech MoUs are a very recent phenomenon — the first one was signed by the Australian Securities and Investments Commission (ASIC) and the UK's Financial Conduct Authority (FCA) in March 2016. Over 30 Fintech MoUs have since been signed by regulators including the FCA, ASIC, the Monetary Authority of Singapore (MAS), the Hong Kong Monetary Authority (HKMA), and the council of the securities regulators of Canada's provinces and territories, Canadian Securities Administrators (CSA)."[53]

In parallel, the international authorities' associations – BCBS, International Organisation of Securities Commissions (IOSCO), International Association of Insurance Supervisors (IAIS), Financial Stability Board, International Monetary Fund – have all engaged in promoting a coordinating evaluation of fintech. Indeed, this project is part of this global exercise. Many of their documents and statements have been referred to in previous documents in this project.

A relevant initiative has been the creation of the Global Financial Innovation Network. Initially a proposal by the United Kingdom's Financial Conduct Authority to explore the feasibility of a *"global sandbox,"*[54] it was later endorsed by another ten regulators, *"to bring the regulatory sandbox concept to a global level (...) into a more structured initiative with the objective of creating a network of regulators who share experiences, collaborate on policy work and regulatory trials and support companies in conducting cross-border tests of innovations."*[55]

50 Bank for International Settlements. BIS Quarterly Review. September 2018.
51 Liu, J. The Dramatic Rise and Fall of P2P Lending in China. In: TechCrunch. August 2018.
52 Bank for International Settlements. BIS Quarterly Review. September 2018.
53 Bromberg, L, Godwin, A. and Ramsay, I. Cross-Border Cooperation in Financial Regulation: Crossing the Fintech Bridge. In Columbia Law School Blog on Corporations and Capital Markets. February 2018.
54 Financial Conduct Authority. Global sandbox. February 14th, 2018.
55 Jenik, Ivo. Global Financial Innovation Network: Not Global Yet. November 2018.

Beyond sharing experiences, developing common definitions and the search for compatible policy approaches, it is important to ensure that whenever a supervisor identifies financial services provided by firms without a local presence, this supervisor can contact not only its counterpart in the financial sector but also other authorities, if the firm is not a regulated financial institution in its home country. Thus, collaboration between authorities should be flexible enough to accommodate requests that may not be explicitly stipulated in formal agreements.

It should be noted that the most prolific advocate of fintech-related MOUs, the Monetary Authority of Singapore (MAS), apparently sees these agreements as part of that nation's drive to position itself as the world's fintech hub. A close examination of some MOUs signed with neighbouring countries shows that the text goes beyond the usual information-sharing and assistance in enforcing provisions, including mutual recognition clauses. *"The mutual recognition aspect implicit in Fintech MoUs is that, if a business meets the regulatory requirements for support to be provided by its home regulator, it is eligible to receive support from the foreign authority that is party to the MoU if a referral takes place — even where there are differences between their respective regulatory requirement."*[56]

In this aspect, the international cooperation prerequisite for a responsible, transparent and competitive implementation of fintech in the financial market is adequately served by information sharing and enforcement assistance, as described by BCBS Principle 3: Cooperation and collaboration. Arrangements will need to ensure confidential information is protected and will only be used for a specific identified purpose. However, the inclusion of mutual recognition clauses in a cooperation agreement, given the huge disparities in regulatory requirements and supervisory capabilities between countries, could potentially undermine the benefits of such agreements.

The financial authorities have regular informative channels with the judiciary

Financial authorities' decisions are often subject to legal redress by those affected. As with any other agency, the supervisor must be accountable to those affected by its decision. The financial legislation usually provides the supervisor with ample powers to act to prevent or mitigate customers' financial losses, as well as to avoid economic damages from widespread instability. Therefore, any judicial recourse by firms and individuals takes place ex-post.

"Courts, in practice, exercise restraint and defer to the expert knowledge of the supervisor, given that they do not normally possess the expertise in financial matters. Substantive accountability is, therefore, of less significance, and judicial review is generally limited to review of legality with a view to ensuring that discretion is not exercised in bad faith or for improper purposes."[57]

For traditional finance this approach works generally well. With the advent of fintech however, authorities could be compelled to act even in cases where either the product, service or process is not explicitly defined in the legal text as financial or the provider claims its business activities are not within the supervisor's scope.

Fintech products usually involve a combination of technologies and business models that are not necessarily associated with traditional finance. This creates the risk that the connection of a fintech product with financial services is not immediately clear to an outside observer, such as a judge.

A good example of this has been the treatment of cryptoassets in courts. Given that even within financial authorities there have been differing views on how to categorize cryptoassets and the absence of a specific law anywhere, it is not surprising that courts also differ in their treatment.

So far most regulatory actions have been confirmed by the courts. However, it should be noted that it took three

56 Idem.

57 Hüpke, E., Quintyn, M, and Taylor, M.W. The Accountability of Financial Sector Supervisors: Principles and Practice. IMF Working Paper WP/05/51. March 2005.

years for the US Commodity Futures Trading Commission to have its categorization of a cryptoasset as *"a commodity covered by the commodity exchange act"*[58] confirmed by a court.[59]

This episode, consistent with CPEBS Principle 8, highlights the usefulness of providing the judiciary with relevant information before a case is heard, as it should allow a speedier and informed process.

Another relevant aspect of this communication is the applicability and use of crisis management frameworks and resolution regimes, where the judiciary has a relevant role, to minimize potential disruptions to financial stability arising from fintech distress.

The country has a national financial inclusion policy or similar instrument that treats fintech as an important tool

Promoting financial inclusion has become a national policy in most developing countries, prompted by concerted policy declarations by the G20, the World Bank and other international bodies. The founding of the Alliance for Financial Inclusion in 2008 by a group of developing countries' central banks[60] allowed for systematic and constant effort towards the goal of bringing access to financial services to the still-unbanked. It was followed shortly thereafter by the creation of the Financial Inclusion Experts Group and the Global Partnership for Financial Inclusion (GPFI) by the G20 in 2009 and 2019, respectively. One of the main recommendations of these bodies was for countries with high levels of financial exclusion to establish a national financial inclusion strategy (NFIS). By December 2017, 9 of 22 countries in Latin America and the Caribbean reported that they had such strategies, while another 6 indicated one was in development.[61]

Alternatively, some countries have enacted laws specific to financial inclusion, while others have issued policy statements. The key is *"to have a strong political commitment and coordination across relevant public and private stakeholders and be able to create an enabling environment and wide-reaching policies that promote responsible financial access, financial capability, innovative products and delivery mechanisms, and high-quality data to inform policy-making."*[62]

By 2016, analysis of the main drivers of the notable reduction of the unbanked in the last 10 years revealed the significant role of fintech products in this achievement. This led the GPFI to *"formally recognize digital financial solutions as critical tools in facilitating global financial inclusion"*,[63] and to issue a set of principles for digital financial inclusion.[64]

The combination of a NFIS or similar instrument with high political profile, usually with access to local and foreign funding for associated projects, and the realization that fintech products have proven impact in advancing financial inclusion, should result in an enabling environment for the development of fintech products more likely to have the desired attributes once introduced in the financial market.

It should be noted that in most LAC countries with or planning NFISs, the financial regulator coordinates the implementation. However, more than half of the region's ASBA members either did not have a NFIS or did not respond to the survey, a likely indicator that there is no NFIS in place.

Based on reports from the international bodies promoting financial inclusion, the decision to engage in a NFIS requires the active commitment of the highest levels of government, thus it is not within the sole remit of the financial regulator. Therefore, this condition must be considered a prerequisite.

58 Commodity Futures Trading Commission. CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering. September 2015.
59 CFTC. Federal Court in New York Enters Preliminary Injunction Order. March 2018.
60 Initially those belonging to the G24, including 10 from LAC.
61 World Bank. Global Financial Inclusion and Consumer Protection (FICP) Survey. December 2017.
62 World Bank. Financial Inclusion. October 2018.
63 Alliance for Financial Inclusion. Fintech for Financial Inclusion: A Framework for Digital Financial Transformation. September 2018.
64 GPFI. G20 High-Level Principles for Digital Financial Inclusion. 2016.

PART 2

GUIDELINES FOR THE REGULATION AND SUPERVISIONOF TECHNOLOGICAL FINANCIAL INNOVATIONS

INTRODUCTION

Part 2 contains a set of regulatory guidelines and supervisory practices for fintech products, services and business models (henceforth "fintech products"),[65] which financial authorities can use to select the appropriate responses to fintech developments in their jurisdictions.

These guidelines allow authorities operating under different legal systems, any stage of financial system development and any level of fintech activity to obtain useful insight on how to conduct an internal discussion when dealing with specific fintech issues. This approach reflects the fact that fintech developments are recent, thus financial authorities worldwide are adopting dissimilar regulatory and supervisory actions.

These guidelines are particularly targeted to those involved in designing and proposing fintech strategies and specific actions within ASBA member countries. Nevertheless, it could also help other authorities within each jurisdiction to understand the interactions between financial segments and the broader effects that fintech can have beyond the usual financial regulatory and supervisory perimeters.

Each guideline begins with a brief overview of the topic, followed by a description of the elements that financial authorities should evaluate when defining adequate responses to the introduction of technological innovations in their financial markets. Then, the guidelines provide a menu of possible regulatory and supervisory actions, drawn from practices identified by financial authorities with significant fintech developments. Every guideline is self-contained and can be read independently, allowing the reader to directly access the topics relevant in her/his jurisdiction.

These guidelines must not be understood as best practices or principles, as fintech is an evolving area, with new developments continuously hitting the markets. In particular, the convergence of Big Tech and finance is being recognised as a potential game changer by traditional financial institutions and governments worldwide. Therefore, financial regulation and supervisory practices are still changing to adapt to those developments.

The structure of this section is as follows: Chapter II contains guidelines on general fintech topics, including general policy approach, regulatory perimeter and supervisory powers, cooperation framework, licensing, fintech knowledge enhancing tools, technology and cybersecurity risks as well non-prudential issues such as AML/CFT.

Chapter III contains guidelines regarding specific fintech products, arranged in sets according to their characteristics. Chapter IV (Annex 1) contains a list of the fintech products considered while preparing the guidelines, as well as a brief description.

65 In this document, fintech is defined broadly, taking into account Big Techs and enabling technologies thoroughly tied to financial services.

GENERAL TOPIC GUIDELINES

This chapter presents a set of guides aimed at supporting the authority's decision-making process in reviewing and designing general strategies and regulatory and supervisory actions as a response to the introduction of technological innovations in the financial market. Even though there are marked differences between various products, services or business models associated with technological innovations, these guides cover a wide range of topics that span all fintech products.

Each guideline starts with an overview of the issues discussed, providing background, developments in financial markets with significant large fintech activity and policy issues raised by international organisations. The next section provides a list of topics that the reader should evaluate, in the context of current conditions and potential developments in the jurisdiction. In most cases, this section presents developments or conditions that may be arising - or will likely arise - in the jurisdiction.

The following section presents a menu of possible supervisory and regulatory actions, drawn from recommendation by international organisations and from the practices observed in jurisdictions with an active fintech landscape. Nevertheless, the reader should primarily use the results of the evaluation of the topics listed in the second section to determine which among the actions presented are the most suitable for their jurisdiction.

GUIDELINE No 1
GENERAL FINTECH POLICY APPROACH

Related fintech products

All

1 Overview

There is a consensus that fintech[66] developments may foster more competitive, inclusive and efficient *financial* markets.[67] However, as noted by the Financial Stability Board (FSB): *"although greater competition can create a more efficient and resilient financial system, heightened competition could also put pressure on financial institutions' profitability and lead to additional risk taking among incumbents in order to maintain margins."*[68]

Furthermore, participation by Big Tech firms may not result in a more competitive market over the longer term as they could achieve scale very quickly with the possibility that cross-subsidisation allows lower operating margins and gaining greater market share. Studies find that both very concentrated markets and very strong competition can be tied to systemic risks.[69]

Therefore, a successful introduction of these financial innovations is not something that can be considered as an accomplished fact.

First, financial systems, in general and in Latin America and the Caribbean in particular, may be characterized by a market structure that severely restricts the ability of new companies to achieve a secure and sustainable position in the market.

Second, technological innovations by themselves are not inherently favourable or detrimental. However, if the associated emerging risks are not properly managed, these innovations can lead to financial instability and/or result in harm to financial service consumers.

Last but not least, the supervisor may become aware of developments in the financial sphere of which it has no prior expertise or knowledge.

This backdrop has induced some financial authorities to adopt a proactive policy stance towards fintech. However, not every regulator or supervisor has adopted such a position.[70]

2 Evaluation topics

This section provides a list of topics that the reader should evaluate, in the context of current conditions and potential developments in the jurisdiction. In most cases, this evaluation topics present developments or conditions that may be arising —or will likely arise— in the jurisdiction.

2.1 Market structure

The financial system can be characterised as an oligopoly, with significant barriers to entry. For example, no very new

66 "FinTech is defined 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." Financial Stability Board. Financial Stability Implications from FinTech. June 2017.

67 As demonstrated by statements by the Financial Stability Board, the Basel Committee on Banking Supervision, the International Monetary Fund, among several international and national public authorities.

68 Financial Stability Institute. FinTech and market structure in financial services: Market developments and potential financial stability implications". 14 Feb 2019.

69 Idem.

70 ASBA. Identifying Gaps and Opportunities in Financial Innovation Regulation - Final Report. 20 April 2018.

competitors (or few) have successfully entered the market in the last 10 years.

Prices (interest rates and fees) are unresponsive to cost-reducing technological advances and are homogeneous across the market.

Interest rate gaps and fee levels are higher than in comparable jurisdictions.

Fintech products are being introduced by incumbent financial institutions without the beneficial effects seen elsewhere. For example, incumbents provide mobile money services, but users pay similar fees as before.

Small fintech firms or entrepreneurs struggle to reach users directly as incumbent financial institutions block access or charge very high fees for required services, such as deposit accounts or trusts.[71]

Fintech firms claim incumbents are blocking their activities. For example, the sandbox experience of the Financial Conduct Authority in the UK documents incumbents' refusals to open payment accounts for fintechs without disclosing the actual reason for such rejections.

Incumbent financial institutions claim fintech firms are operating in disregard of current regulation.

There is a significant lack of financial inclusion, at the jurisdiction level, in specific geographic areas or among certain demographic groups, due to gender, age or ethnicity.

Traditional financial institutions offer limited services, including lending, to small and medium-sized enterprises (SMEs) or entrepreneurs, especially in rural locations.

Financially excluded sectors access financial services provided by informal providers (non-fintech).

71 The same cannot be said for Big Tech firms, as they typically have large, established customer networks and enjoy name recognition and trust.

2.2 Legal framework

The existing legal framework is not flexible enough to accommodate technological financial innovations in the market.[72]

The legal framework is unclear regarding the introduction of new fintech products and/or their provision by new firms.Current legal requirements are not suited to financial service provision through digital channels.

Key financial notions, such as what constitutes a deposit or financial intermediation, are not flexible enough in financial laws to encompass new business models and products based on technological innovations.

2.3 Risky, unregulated financial services

Fintech products are being offered in the market by unregulated firms.

There is a significant volume of fintech products provided remotely by firms from outside the jurisdiction.

Consumers are not able to adequately discern whether a financial product or service is provided by a locally regulated financial institution or by an unregulated company, or located within the jurisdiction or overseas.

Consumers have suffered losses by using unregulated fintech product providers.

Fintech products developed in other jurisdictions, not necessarily by regulated financial institutions, are being implemented by regulated domestic financial institutions.

Management at traditional financial institutions has not grasped the full impact of implemented fintech products in their risk management processes.

72 This apparent issue could arise from a lack of information and understanding of the product to make a determination on the accommodations within the ambit of the existing framework, rather than outright inadequacy of the framework.

2.4 Authorities' knowledge gap

The supervisor recognizes it does not have full understanding of fintech products being implemented by supervised financial institutions.

Supervised financial institutions request clarifications from the supervisor on the application of current regulations to innovative products and services.

Other authorities within the same jurisdiction are asking the supervisor about new products and players.

Other authorities in the region are issuing regulations on fintech products and/or authorising providers, not adequately covered by local regulations.

3 Potential regulatory and supervisory actions

Below are the different options for action that an authority can take with respect to fintech. These actions are not mutually exclusive. In addition, the authority may decide to apply one action only to certain types of products but prefer others for different categories of fintech products.

3.1 Wait and see

The supervisor opts for not intervening in the development of fintech initiatives, allowing the market to define which will succeed. These initiatives will have to comply with existing regulations and will be subject to the current supervisory scheme, although the existing legal framework may be deemed inadequate to accommodate these innovations.

However, it should be noted this course of action entails explicit risks for the financial authority, as unsupervised fintech products may cause harm to consumers. Even in jurisdictions with no overt fintech activity, related products may be offered remotely from other jurisdictions.

Furthermore, if there are unregulated fintech activities as described in 2.3, this option may be inconsistent with the authority's mandate.

3.2 Explicit fintech promotion policy

If, after the analysis of the topics presented in subsection 2.1, the financial authority determines that its goals, such as promoting greater competition, financial stability etcetera, are better achieved with an active fintech ecosystem, it may consider spelling out an explicit policy of fintech promotion, complemented by other actions in this guideline as well as tools described in other guidelines.

This policy will usually be a part of a wider public sector strategy towards specific aims, such as competitive financial markets, financial inclusion, enhancing the technological sector, increasing the jurisdiction's attractiveness to foreign direct investment, among others.

The authority's statement will delineate its policy regarding possible regulatory changes, encouragement for new financial services or related fintech providers, its expectations regarding the impact of innovations on prices and safeguards regarding financial consumer protection.

Having a fintech promotion policy does not preclude issuing warnings to the general public on the risks of engaging with non-local providers, unregulated/unregistered domestic providers and riskier fintech products.

3.3 Set up a fintech group

Subject to staff and budgetary constraints, a dedicated fintech group could help bridge any existing knowledge gaps and thus allow the authority to reach informed decisions regarding fintech-related queries or events.

This group or unit conducts research on relevant topics, documents fintech activity in the jurisdiction and elsewhere and acts as the contact point on fintech-related topics for unsupervised firms, users and regulated financial institutions.

Other tasks are to identify new products, new players and new technologies in the market. The unit will prepare an evaluation report including relevant details, innovations with respect to previously identified products

or technologies, an initial regulatory evaluation and recommended course of action.

The unit scope should include cross-border provision of new fintech products to local customers, either taking place already or highly likely to in the near future.

This action is highly recommended in every case, especially when one or more of the elements presented in 2.3 and 2.4 are present in the jurisdiction.

3.4 Fintech stakeholder meetings

The financial supervisor convenes all relevant parties – regulated financial institutions, fintech players, technology providers, MNOs and others – to discuss relevant issues. These meetings could have a formal setting with a defined periodicity or be convened for specific issues. They usually include other authorities, within the cooperation framework described in 3.6.

The supervisor sets the agenda for discussion, based on prior research, and describes potential initiatives it is studying. Although the supervisor will be open to receiving suggestions, comments and proposals from the stakeholders, these meetings should not be considered as an instance to formulate regulations or supervision policies. This must be explicitly stated in terms of reference so as not to allow for misinterpretation by any party.

These meetings can evolve to become Innovation Hubs, fully described in Guideline No 5 - 3.2.

3.5 Propose changes to the legal framework

If, as a result of the evaluation in subsection 2.2, the authority concludes that fintech services, products and business models may not be adequately covered by existing regulation and/or that the powers granted by law to the supervisor may restrict its ability to prevent harmful activities beyond its remit, a sensible course of action may be to propose changes to the laws governing financial activities and defining the power of the financial authority.

Giving the evolving nature of fintech products and the lack of internationally agreed-upon best practices, any legislative action should aim to set high-level principles or definitions, providing the financial authority sufficient leeway to adapt, via regulation or supervisory policies, specific details.

In any case, legal changes must be carefully considered to avoid stifling innovation or the supervisor's powers by setting rigid requirements or definitions.

3.6 Coordinated public sector fintech position

The financial supervisor promotes a cooperation framework among public sector authorities in relation to fintech. This coordination effort usually includes, depending on the jurisdiction's characteristics, the central bank, other financial regulators, the consumer protection agency, the telecommunications regulator and other relevant public sector authorities.

The goal of this coordinating effort is to ensure a coherent approach to fintech, reducing possible regulatory gaps, aligning priorities and safeguarding the interest of financial users. Further details are presented in Guideline No 3 - 3.2.

3.7 Evaluation of possible anti-competitive behaviour actions

The supervisor, upon gathering evidence of activities by regulated financial institutions that impede or restrict the offering of fintech products by new competitors or any uncompetitive outcome from the introduction of fintech products., defines a proportionate response, in accordance with local legal and institutional arrangements.

In some cases, anti-competitive actions are directly a result of current regulations, in which case the authority should consider changing the rules to avoid their use as barriers to new players in the financial market. These actions should be framed within a set of principles aimed at fostering a more competitive, inclusive and efficient financial system.

GUIDELINE No 2
FINTECH REGULATORY PERIMETER AND SUPERVISORY POWERS

Related fintech products: All

1 Overview

The arrival of new financial products, services and business models into the market has upended the existing regulatory framework, designed with a traditional banking model in mind. It is also testing the limits of supervisors' capabilities to ensure financial stability and good market conduct within their jurisdictions.

It is important to bear in mind that fintech can enter the financial market through four different channels:

a) New firms (start-ups) with no prior financial experience;
b) Existing (regulated) financial institutions;
c) Existing local non-financial companies with a large customer base;[73] and
d) Firms located outside the jurisdiction, offering fintech products remotely to local customers.

It is also possible for fintech products to be introduced through a combination of these channels, such as traditional financial institutions establishing partnerships with fintech start-ups or large foreign non-financial companies providing fintech products remotely.

Each modality presents unique challenges to the authorities and usually requires different approaches, consistent with the powers granted by legislation.

Also, it could be the case that authorities are unfamiliar with fintech products, making it harder to decide whether current regulations apply and which supervisory stance to adopt. This knowledge gap is addressed in Guideline No 5, therefore, in this guideline it assumed that the authority has taken adequate actions to reduce that gap.

At the same time, fintech dynamics stimulate the accelerated introduction of innovations to take advantage of their commercial impact before they can be replicated by competitors. This can induce fintech providers, new to financial markets, to overlook some of the usual risk management steps taken by regulated financial institutions when introducing new services or products. Even traditional financial institutions may fail to carry out appropriate analysis and adopt mitigation actions when introducing fintech products. That could translate in unsafe provision of financial services as well as possible breaches of legal restrictions.

In this context, it is possible that the authority felt compelled to act, either by issuing or amending regulations or by taking preventive or corrective actions, but lacks certainty on whether these actions fall within its remit. Although a possible avenue to addressing this situation is to propose and obtain explicit new powers through primary legislation, as indicated in Guideline No 1, this guideline is designed to guide the authority while exploring potential legally viable options.

It is important to highlight that given the still-evolving fintech ecosystem, any such legislative action could rapidly become obsolete or too rigid. This concern can be overcome in the case of jurisdictions where the legal system allows for a principles-based approach to financial regulation and supervision. Nevertheless, as legislative processes are uncertain and usually disconnected from

73 Generally, MNOs or 'Big Tech' firms: online shopping platforms or social media companies.

financial authorities' urgencies, it is highly convenient to examine the choices available to tackle emerging dangers in the financial markets.

A crucial issue in this context is the erosion of the borderlines of what constitutes a deposit. Most legal frameworks focus on activities involving the handling of customer funds and subsequently transferring those funds to other customers; that is financial intermediation. However, fintech products sometimes blur the line between simple money storage or safekeeping and a deposit.

In this sense, fintechs may be said to engage in deposit taking during the periods when they retain their customers' money for purposes of onward transfer, as well as when their customers decide to retain money on their prepaid cards. Thus, given that the banking statute of numerous nations stipulate that banks are the only institutions authorized to engage in the business of deposit taking, it could be surmised that fintechs are in violation of the law, which illustrates the legal difficulty associated with fintech regulation.

Moreover, traditional boundaries between direct intermediation, as when an investor buys a company stock and in indirect intermediation typical of banks, are increasingly difficult to apply to some fintech products. At the same time, some fintech firms seem reluctant to define their services as financial intermediation. Thus, deciding whether fintech products lie within the regulatory perimeter may often involve interpreting the legal definitions of deposits and financial intermediation.

Another growing area of concern for financial authorities and international bodies[74] is large non-financial companies (fundamentally Big Tech firms and to a lesser extent MNOs) becoming key players in the financial market, either by providing technological services essential to market infrastructure, or as fintech product providers.

As providers of essential technological services, these large companies in fact are the main enablers of most fintech products. Without stable data networks, mobile phones services, cloud services and data gathering and processing, many fintech providers would not be able to function. This reliance extends to traditional financial institutions looking to reduce fixed costs, by promoting remote digital access to their services to allow for drastic reduction in their branch networks.

As financial service providers, these companies have the potential to alter dynamics in financial markets at any moment. Although at present these companies have been cautious in competing openly with traditional financial institutions, experience in those jurisdictions where Big Tech and MNOs provide the full range of financial services (most notably China) shows that they can rapidly reach a sizeable market share, overshadowing traditional financial institutions.

2 Evaluation topics

2.1 Unregulated financial service provision

Incumbent financial institutions are asking the supervisor to stop unregulated fintech competitors, claiming they enjoy a competitive advantage by providing regulated services or products.

Operating fintech product providers are approaching the authority for regulatory interpretation and possible licensing options. However, their products are not clearly defined in the regulations.

Unregulated firms offer P2P and equity crowdfunding products, claiming that no financial intermediation occurs as "investors" take all the risks and receive no guarantee of a return on capital nor of interest.

74 Financial Stability Board. Fintech and Market Structure in Financial Services. February 2019.

Unregulated firms operate payment and digital wallet products, claiming they do not breach legal or regulatory restrictions as they operate within a closed group.

Unregulated firms may bring into the jurisdiction technological innovations developed abroad, without a proper risk assessment taking into account local conditions.

2.2 Cross-border financial service provision

Local businesses and individuals are able to engage in financial transactions with unregulated providers without a presence in the jurisdiction.

Local unregulated firms grant customers access to financial products provided by foreign companies, either related or unrelated.

Regulated financial institutions provide fintech products that partially rely on services delivered by unregulated foreign-related companies.

2.3 Fintech developments by large non-financial companies

Large non-financial companies provide fintech products that individually are not covered by regulations, but taken as a whole replicate regulated financial products or services.[75]

Large non-financial companies offer financial-like services tied to online shopping, such as payments, money storage or lending, either independently or in association with regulated financial institutions.

Large non-financial companies facilitate access to lending products based on data gathered from customers.

Large non-financial companies, looking to become financial services providers, also play a key role in the provision of essential financial market infrastructure services, such as cloud computing or data networks.

2.4 Introduction of fintech products

Regulated financial service providers are able to introduce technological innovations, developed in-house, locally or by a parent abroad, or purchased from other firms, without engaging in a risk assessment.

Regulated financial institutions are not required to notify or provide detailed information to the supervisor before implementing a new fintech product.

Financial sector trade bodies do not engage regularly with the supervisor when discussing technological changes to key financial infrastructure services or wholesale market platforms.

The financial system has a fintech skills shortage, expressed in high turnover and capture by non-financial firms.

Top executives and board members at regulated financial institutions do not usually possess technological skills commensurate with the increased reliance on technology.

3 Potential regulatory and supervisory actions

3.1 Evaluate the economic substance of fintech products

The regulator, having identified activities such as those described in subsections 2.1, 2.2 and 2.3, proceeds to evaluate whether the fintech product provided is, fundamentally, a regulated financial service or product, offered by unregulated firms.

If the conclusion is yes, then it proceeds to assess the applicability of the current legal framework. The analysis should include the potential benefits or risks inherent to

75 For example, an MNO offers prepaid airtime and airtime balance transfers between customers, allows the purchase of goods and services using airtime balances and lends airtime credit in exchange for a "service fee," as separate products.

the product and whether or not it is appropriate to try to regulate the activity.

Although international organisations have recommended a *"more activities-based rather than entity-based"*[76] fintech regulatory approach, most financial sector laws take the opposite view. Therefore, the evaluation most probably will focus on whether the firms providing fintech products are within the regulatory perimeter or not.

Depending on the legal system and the specific provisions of the law governing financial activities, there are at least three possible scenarios:

a) Fintech products offered by unregulated fintech providers are sufficiently similar to those provided by regulated financial institutions, as defined in the legal framework. Therefore, these providers are engaged in unlicensed activities. Authorities must define how to determine what is "sufficiently similar."
b) The governing law allows the regulator to interpret its definitions. Thus, the regulator can expand the regulatory perimeter and demand unlicensed providers to become regulated entities.
c) It is not possible to extend the regulatory perimeter to include fintech providers not defined in the current legal framework.

It should be noted that this evaluation must be performed for the providers of each class of fintech products, and thus the resulting scenario may differ among them. Once this evaluation is done, the financial authority has several possible courses of actions, as described in the following points.

3.2 Enlarge the regulatory perimeter

The financial authority, after evaluating a fintech product and its providers, finds it falls in the scenario described in 3.1 b). Also, the regulator decides that is convenient to encompass the providers within the regulatory perimeter, based on the financial authority's legal duties and the application of the core principles for effective banking supervision.

The regulator proceeds to determine whether the current regulations adequately cover that fintech business model or if new regulations or changes to existing ones are required. Then, it informs the fintech providers that they must apply for an authorisation within the current licensing arrangement or under a special scheme, as described in Guideline No 4.

Furthermore, the regulator must define terms critical to the functioning of financial systems. For example, in several jurisdictions, a legal definition of financial intermediation does not exist. This could be compensated for if the supervisor has the power to deem something as such and treat the product accordingly.

3.3 Tackling unlicensed provision of fintech products

While, under the scenario described in 3.1 a), the supervisor should treat unlicensed fintech providers similarly to any other firm offering financial services without the required authorisations, the authority may find it advisable to evaluate whether the provider is breaching the legislation because there is no viable way to conduct their activities under the current legal framework.

The supervisor, following a close examination of providers of specific fintech products, may conclude that there are compelling reasons not to prevent the provision of an innovative financial service, but that it is preferable to drive the unlicensed providers towards adopting a legal form conducive to obtaining a licence. In this evaluation the supervisor takes into account what benefits the related fintech product may bring to the the financial market, in terms of greater competition, enhancing financial stability, improving the quality of financial services, financial inclusion, consumer protection or enhancing financial sector integrity, among others. The specific options regarding licensing are discussed in Guideline No 4.

76 Financial Stability Board. Financial Stability Implications from Fintech. June 2017.

If the supervisor reaches a different conclusion, either because the fintech product is potentially harmful to its users or because there is not enough evidence of its potential benefits, an intensive dialogue with potentially harmful providers will be fundamental to understanding the business model and reaching a more comprehensive conclusion.

3.4 Issue public warnings on unregulated fintech providers and products

The supervisor finds it cannot legally bring unregulated fintech providers and their products within the regulatory perimeter, the scenario described in 3.1 c), or that the characteristics of the fintech product has negative implications for financial stability, transparency or consumers.

In this scenario, the financial authority lacks the powers to enforce a cessation of activities by the unlicensed fintech providers. Therefore, in order to mitigate the potential harm to users, the supervisor issues public warnings about the risks involving these products and the unregulated nature of their providers.

Any financial regulator should be in a position to indicate whether or not it regulates a specific provider, mainly through advisories, warnings or public statements on the websites of relevant authorities.

The financial authority can, in parallel, use complementary actions such as proposing legislative changes, as described in Guideline No 1 - 3.5, to close any enforcement gap.

3.5 Enforce cease and desist orders

The financial authority has determined that the fintech product harms consumers or introduces unwelcome risks to the financial market or the wider economy while its purported benefits are small or absent.

The financial authority, usually in parallel with the previous action, enforces a cessation of the activities of the unregulated provider of such a fintech product or, if the provider is a regulated entity, orders a stop to its provision.

The authority should keep in mind that enforcing this action could be very difficult when the fintech product's provision takes place remotely or beyond the legal remit. Therefore, this action may require a coordinated effort with other authorities, as defined in Guideline No 3.

3.6 The supervisor refers its conclusions to another authority

The financial supervisor, having concluded that a fintech product and its providers fall within the regulatory perimeter of another authority, notifies that authority about its findings. A set of mechanisms must be established to resolve controversies in the event that the other authority disagrees with the conclusion.

This action may be part of the cooperation frameworks described in Guideline No 3.

3.7 Supervisory actions regarding cross-border provisioning by unregulated foreign firms

The supervisor, having identified that firms located outside its jurisdiction are providing fintech products to local customers, and that the firms are not regulated as financial institutions in their country of origin, have the following options to mitigate the risks to customers and the potentially damaging reputational effects on the jurisdiction's financial market:

a) The supervisor issues public warnings, similar to those described in 3.4, stressing that in addition to the usual risks involved in dealing with unregulated entities, customers also face currency, political and money laundering/finance of terrorism risks;
b) The supervisor orders regulated financial institutions to treat any transaction with the identified providers as suspected transactions, according to the AML/CFT regulations;
c) The supervisor engages with its counterpart in the provider'scountry of origin to explore common actions within a cooperation framework, as described in Guideline No 3.

These options are also applicable when unregulated local firms distribute fintech products provided by unregulated foreign companies.

In the case of regulated financial institutions that provide fintech products while partially relying on services delivered by unregulated foreign-related companies, the standard outsourcing regulations should apply.

3.8 Require new fintech product assessments

If, from the evaluation of the topics presented in subsection 2.4, the authority perceives it is possible that new fintech products are introduced without proper risk assessments by the providers, the regulator proceeds to amended the regulations to include, if absent, an explicit requirement to analyse, within its risk management process, the impact of the introduction of every new technological innovation on the risk profile of the financial institution.

The financial institution must have a documented, repeatable, and auditable process, approved by the board of directors, to guide their decision to launch the new product or service. Management and staff from relevant areas must participate in these assessments.

The process must ensure that all policies and procedures impacted by the innovation are updated and that there is ongoing evaluation throughout the product lifecycle.

If the technological innovation was developed and implemented initially by a financial group in another jurisdiction, the locally regulated financial institution must analyse whether the technological innovation fits with the local market conditions and the business model complies with the local regulatory framework. The assessment must consider whether the implementing institution's staff have the appropriate skills to detect any deviation from original expectations and to modify the product accordingly. Alternatively, staff training must be part of the implementation procedure.

The supervisor must expect that the regulated financial institution's top management has the power to delay or decline to introduce an innovation or to demand changes to adapt it to local conditions, especially in cases where it belongs to a global financial group.

3.9 Require prior notification for technological innovation implementations

When the elements presented in subsection 2.4 are present in the jurisdiction, regulated financial institutions, including fintech firms, are required to provide the supervisor with advanced notice of the introduction of any fintech product. The notification must include a description of the innovation, any relevant experience in other jurisdictions, the assessments carried out locally and the board or top management's approval document.

The supervisor should have the power to order a delay in the introduction of the innovations. In doing so, the supervisor will provide the motivation and the changes needed. If the supervisor lacks the legal powers to block the implementation, it will take into account the perceived increase in the financial institution's risk profile.

This requirement should extend to technological innovations that introduce changes to the way financial institutions interact with each other, in transactional platforms and other system-wide schemes. In these cases, it is possible that the supervisor engages with other authorities, such as the central bank if it is an independent entity.

3.10 Ensure adequate technological skills at fintech product providers

The supervisor, as part of its regular risk assessments, analyses if the technological skills of management and board members are consistent with the significance of fintech products in a financial institution's portfolio.

The supervisor should be able to order remedial actions if the expected level of relevant skills is insufficient, such as bringing in new individuals with relevant expertise, mandating training or asking for a delay in the introduction of new fintech products until the skills gap is eliminated.

3.11 Promote fintech skills

If, from the evaluation of subsection 2.4 and in accordance with supervisory action 3.10, the financial authority determines there is a shortage of the required technological skills among managers and staff at regulated financial institutions, it promotes the development of fintech skills by supporting training and certification schemes by specialised organisations.

The authority should encourage training at all levels of financial institutions, including certification schemes tailored for top management and board members, designed to provide a comprehensive understanding of financial technological innovations, risks involved, their evolution, experiences in the jurisdiction and elsewhere and the role of management in monitoring safe implementation at financial institutions.

GUIDELINE No 3
AUTHORITIES COOPERATION FRAMEWORK

Related fintech products: All

1 Overview

Fintech products and the firms providing them have proved tricky to categorize within the traditional boundaries that define financial activities. In jurisdictions where the regulation and supervision of financial markets are segmented –independent banking, insurance, capital markets and pension authorities – it is possible that different views may arise regarding which organisation is responsible for a fintech product or provider. It may be even the case that none has a clear mandate to regulate that fintech product or provider.

From a different perspective, many fintech products can be delivered to customers remotely, removing the need for providers to have a physical presence in markets they serve. Yet, at the same time, those fintech products may have negative outcomes in the jurisdiction, not least financial losses to their customers, with detrimental effects on the authorities' reputations. Furthermore, divergent definitions and views on fintech may also arise between jurisdictions.

To mitigate these risks and to improve regulatory and supervisory efforts regarding fintech activities, existing cooperation agreements must be enhanced. The Financial Stability Board has identified[77] three priority areas for international cooperation: managing operational risks from third-party service providers, mitigating cyber risks and monitoring macro financial risks. The international organisation also highlighted, among other issues that merit authorities' attention, the need to further develop open lines of communication across relevant authorities to deal with emerging cross-border legal issues and regulatory arrangements. This view is shared by the Basel Committee on Banking Supervision in its call for closer cooperation between authorities, within jurisdictions and across countries, as a necessary step to enhance financial sector safety and soundness given the current and potential global growth of fintech firms.[78]

The goal of this guideline is to facilitate the evaluation of the main issues involving cooperation between authorities, both within a jurisdiction and internationally. Then, it presents a series of potential regulatory and supervisory actions, whose applicability will depend on the specific legal framework and financial supervisory architecture in each jurisdiction.

2 Evaluation topics

2.1 The financial supervision institutional framework

The laws governing financial activities set boundaries between different financial authorities' remit based on fixed definitions of entities and the activities in which each type is allowed to engage.

Coordination and cooperation mechanisms among those authorities are not well developed or are slow to respond to emerging issues.

77 Financial Stability Board. Financial Stability Implications from Fintech. June 2017.

78 Basel Committee on Banking Supervision. Implications of Fintech Developments for Banks and Bank Supervisors. February 2018.

Financial authorities pursue potentially conflicting goals, for instance, fostering competition, ensuring key players financial stability, consumer protection.

2.2 Cooperation between financial authorities and other relevant non-financial regulators

The legal framework does not foresee cooperation schemes among financial and non-financial authorities.

There has been little or no experiences of informal coordination or cooperation between financial and non-financial authorities.

Existing regulatory gaps are reinforced by diverging authorities' interpretations of fintech activities.

2.3 Fintech products provided by non-financial firms

Non-financial firms authorised and regulated by a non-financial regulator are providing fintech products beyond the financial supervisor's remit.

It is difficult for customers to distinguish between fintech products provided by a non-financial firm and similar financial services provided by regulated financial institutions.

Existing regulatory gaps mean that customers of fintech products provided by non-financial firms are at risk of suffering financial losses.

Fintech products provided by non-financial firms have more attractive financial terms than similar financial services provided by regulated financial institutions, such as lower fees, quicker settlement, simpler requirements.

2.4 Existing cooperation agreements with international counterparts

Existing memorandums of understanding and other cooperation mechanisms with other financial supervisors only cover information exchange and examiners' access to foreign branches of regulated local financial institutions.

Cooperation agreements are segmented by financial sector, for instance, between banking authorities and insurance regulators. There are no international cross-sectoral cooperation mechanisms. Local cross-sectoral schemes do not cover international issues.

Existing agreements are inflexible, have strict precise definitions of financial activities and entities and do not cover new or slightly different activities or providers.

Existing arrangements do not contemplate assisting the international counterpart to contact other local non-financial authorities.

2.5 Fintech activities straddling sectoral boundaries and international borders

There are fintech products and/or providers with characteristics of financial services of two or more legally distinct financial sectors, for example, crowdfunding platforms combining equity and lending in a single product.

Certain fintech products, such as cryptoassets, remain unregulated in the jurisdiction as no financial authority sees them as within their regulatory perimeter.

Business and individuals in the jurisdiction are customers of fintech providers with no presence in the jurisdiction.

2.6 Fintech developments in other jurisdictions

The authority identifies fintech regulatory developments and supervision practices in another jurisdiction that could be of interest as there are similarities between the financial markets and financial legal framework.

The authority is aware of, or has been approached by, fintech firms authorised in other countries that are exploring conditions to enter the market.

The authority is aware of a fintech product being implemented by the parent company of a financial institution present in the jurisdiction.

The authority is aware of a cross-border fintech product being implemented in another jurisdiction by a group of financial institutions, including one or more with presence in its jurisdiction.

3 Potential regulatory and supervisory actions

3.1 Strengthen coordination and cooperation mechanisms between local financial authorities

To ensure consistent and enforceable policies regarding fintech activities, financial authorities should promote permanent mechanisms to share information, discuss strategies and coordinate actions. This is imperative if the situation described in subsection 2.1 is present in the jurisdiction. It is important than in any initiative to engage fintech stakeholders, as described in Guideline No 1 - 3.4, all financial authorities are included and, if possible, had previously agreed on a common position.

Among the topics that financial authorities should aim, within their statutory duties, to reach a consensus on are:

a) A common set of criteria to identify and classify fintech products and providers;
b) Pooling resources to enrich knowledge of fintech activities;
c) Coordination mechanisms to tackle failing fintech providers.

3.2 Develop coordination mechanisms with local non-financial authorities

Fintech activities are relevant to regulators and public authorities with responsibility in areas such as telecommunications, privacy and data protection, AML/CFT, consumer protection, fair competition, financial inclusion, promotion of micro, small and medium enterprises and national security. Therefore, if the elements described in subsections 2.2, 2.3 and 2.5 are present in the jurisdiction, the financial authorities should take steps to engage with their non-financial counterparts.

By creating a single discussion platform for all the relevant authorities, also described in Guideline No 1 - 3.6, the risks of uncoordinated actions are minimized. Moreover, by sharing information in a timely manner, all authorities would enhance their ability to ensure that all fintech players comply with the respective laws and regulations in each area.

The financial authority should foster agreements among participant in at least the following areas:

a) Acknowledgement by other authorities that fintech products are inherently financial activities.
b) The financial authorities should be the leading enforcer of corrective actions in fintech-related issues.
c) Regulatory gaps and loopholes deriving from divergent financial and non-financial regulations should be closed, giving financial regulations priority if money from the public is involved.
d) Non-financial companies providing fintech products should be compelled to either create separate regulated firms to exclusively provide such fintech products or become regulated financial institutions themselves, depending on the available options, as detailed in Guideline No 4.

Last but not least, for fintech promoters, having a single and unified public sector position provides greater certainty and prompts sounder and more resilient developments.

3.3 Propose fintech cooperation agreements with financial authorities in other jurisdictions

Weaknesses in existing cooperation agreements detected in the evaluation of subsection 2.4 and developments described in subsections 2.5 and 2.6 should encourage the supervisor to contact counterparts in relevant jurisdiction to specifically address fintech activities in cooperation agreements, either by changing existing provisions or drafting a new fintech-specific arrangement.

The target jurisdictions should include, at least, those that have the following characteristics: Important bilateral financial trade flows;

a) Presence of financial institutions with activities in both jurisdictions;
b) Being the country of origin of fintech providers with local customers;
c) Having fintech financial policy developments that are relevant to the authority;
d) Significant migration levels between the two jurisdictions.

The financial authority should aim to include in these fintech cooperation mechanisms, as a minimum, the following provisions:

a) Information exchange on fintech developments;
b) Training opportunities for local staff, if available;
c) Coordination mechanism in case of failing fintech providers;
d) Assistance in requesting support from non-financial authorities in the other jurisdiction in cases of unregulated fintech providers;
e) Assistance when examining key market infrastructure players, such as cloud services;
f) Bilateral assistance when developing fintech knowledge-enhancing tools as described in Guideline No 5;
g) Exploring developing compatible regulations for cross-border fintech products and providers;
h) Joint stance when regulated financial institutions operating in both countries plan to implement technological innovations with significant impact in how they operate, both individually and in inter-institutional transactions.

GUIDELINE No 4
FINTECH LICENSING APPROACH

Related fintech products: All

1 Overview

Financial authorities all over the world have found that certain fintech product providers do not fit in any of the traditional categories for authorisation in existing laws. This has led in some cases to the unlicensed provision of products and services that are very close to, but not exactly the same as the financial activities defined in the legal framework.

Also, fintech developments are allowing new business models in the provision of financial services that are not easily translated into the categories of most legal texts, as these models straddle financial and non-financial activities.

This has prompted some jurisdictions to create new categories of regulated entities, either by developing types under the current legislation or by enshrining specific fintech licences in new legislation. In some cases, the law or the regulator has created short-term financial licences, specifically tailored to test fintech products, with the expectation that at the expiration date, the licensee, if the test is successful, will upgrade to a permanent licence or will cease to operate as an authorised financial firm.

The authority must consider its options regarding licensing in the context of its stance towards fintech, as described in Guideline No 1. The selected fintech policy will inform whether the licensing scheme will provide those interested in becoming providers of fintech products with regulatory advantages with respect to promoters of new traditional financial service providers.

Fintech activities are constantly evolving and it is not yet clear when the range of new products, services or business models enabled by technological innovations will reach a pause. This characteristic means that any decision taken today will probably have to be updated or reviewed in the medium term, either because new fintech products emerge or current business models morph into something different.

Whatever the route chosen, if the regulator finds it necessary to develop a specific fintech licensing scheme, it needs to decide on the differences between the requisites for these new licences and the standard authorisation criteria.

The objective of this guideline is to provide assistance in formulating the main elements of the new scheme. As this is a matter usually reserved to legislative processes, the reader must take into account the relevant features of the jurisdiction.

2 Evaluation topics

2.1 Legal framework flexibility

The legal framework defines a set of regulated activities giving the regulator room to include new ones by interpretation and to define which institutions can engage in those activities.

The regulator's mandate is defined by law in terms of a set of principles allowing the regulator to interpret the law's provisions to adapt to new financial products.

2.2 Financial institution ownership

The law or the regulations sets a minimum number of non-related shareholders at financial institutions.

The law restricts specific categories of companies from becoming controlling shareholders of financial institutions.

2.3 Current licensing scheme

Licensed financial institutions can engage in a diverse range of financial activities.

Aspiring fintech firms find it difficult to become licensed institutions due to onerous requirements (financial and other).

The regulations allow for creating narrowly defined licences, in terms of range of activities, with more flexible or proportionate requirements than regular licences.

2.4 Narrowly defined fintech institutions vs. general digital financial institutions

Most fintech firms in the jurisdiction provide (or wish to provide) a single fintech product or a limited set of fintech products.

Fintech firms in the jurisdiction with single or few permissible activities face increased concentration risks.

Fintech firms in the jurisdiction with a narrow set of products potentially have reduced sources of revenue, impacting their sustainability.

2.5 Fintech general policy

The authorities have adopted a fintech promoting policy including knowledge enhancing tools such as regulatory sandboxes and others explored in Guideline No 5.

Existing licences do not fit well with regulatory sandboxes. In particular, standard licences are not suitable to temporary authorisations.

2.6 Standard requirements in a digital financial landscape

Fintech firms in the jurisdiction operate from rented locales sometimes shared with other firms, rely on cloud services for most if not all their computational processing and data storage needs and do not have physical branches or offices to interact with their customers.

Existing regulations require new institutions to have specific equipment, premises and or procedures before starting operations, which are ill-suited for, or impossible to comply by purely digital financial service providers.

For most potential fintech firms and online-only banks in the jurisdiction, the cost of satisfying these requirements will undermine the business case.

2.7 Corporate culture and customers treatment

Fintech firms' owners and management may have strong technological skills but lack financial expertise.

The customer base profile of a start-up firm may differ from that usually seen in traditional financial services, with a greater share of young and urban clients.

Large non-financial companies usually have customers relationships based on short-term and remote interactions.

Technology firms, of which fintech firms are a subset, tend to prioritise speed and uncluttered detail in transactional interfaces over clear and accurate information.

In some instances, fintech firms may not recommend products and services appropriate to the needs, interests and objectives of customers.

3 Potential regulatory and supervisory actions

3.1 No special licensing schemes

As a result of the evaluation of subsection 2.1, the authority may find it cannot adopt a special licensing scheme until there is a change in the legal framework. In this case it should be noted that the authority must be prepared to either tolerate unregulated fintech activities or to enforce adherence to standard financial legal and regulatory frameworks.

Even if this evaluation has a different result, the authority may decide that there is no convincing case to establish a special authorisation process or to relax the standard requirements for fintech product providers. This stance is especially suited to a wait-and-see fintech policy as described in Guideline No 1 - 3.1.

3.2 Develop a specific fintech licensing scheme

This option presupposes that the regulator is entitled to create a specific fintech licensing scheme, using powers granted in general financial legislation to define new financial services and products provided under an existing licence, as presented in subsection 2.1.

The specific features of the scheme will depend on the authority's evaluation of the topics discussed in subsections 2.4, 2.5, 2.6 and 2.7. The scheme will have at least the following provisions differentiating fintech licences from standard authorisations:

a) Range of activities allowed. These may range from a single fintech product to the full range, as in the case of online banks.
b) Initial capital. A lower minimum amount of initial capital for fintech firms with a narrow range of permitted activities than the standard requirement.
c) Prudential capital level. The capital-to-assets ratio is set below the standard ratio for other financial institutions. Also, the risk weights and ratio components reflect the specific risks and balance composition of fintech firms with limited activities. In particular, risk-mitigating measures such as mandatory separation of clients' funds in a bank deposit or trust in the case of payment and money storage services should be reflected in the capital-to-assets ratio regulation.
d) Ownership. A single non-financial company is allowed to be the only or the controlling shareholder of a fintech firm in order to bring the financial activities of the company within the regulatory perimeter. This does not exempt the firm from providing details of the ultimate beneficiary owners.
e) Board member skills. Firms must have a balanced mix of skills among members of the board, including technological, financial and regulatory expertise, similar to what is demanded of traditional financial institutions.
f) Management. Firms are required to appoint staff at management level with specific financial expertise gained at traditional financial institutions, to complement the technological skills of the promoters. The supervisor must be satisfied that the fintech firm's top management and selected officials have a customer relationship approach consistent with a financial services provider, and that adequate steps have been taken to reinforce this cultural change throughout the firm.
g) Technological resilience. The firms are required to demonstrate their activities can withstand technology-related operational events.

3.3 Time-limited special licence

This is a variant of the previous option. In this case, the authority decides to create a special category of short-term licences, in conjunction with product-specific tests, such as a regulatory sandbox as described in Guideline No 5- 3.5.

In addition to the considerations described in the previous subsection, and in subsections 3.4 and 3.5 of Guideline No 5, the authority ensures that the firm holds enough capital that is easily accessible and unencumbered to return all funds received by clients during the final stages of the test.

The scheme must spell a path to a regular financial license, if the test is completed to the satisfaction and the firm, owners and management fulfil the usual regulatory requirements to obtain a license.

Likewise, the authority must be able to withdraw the licence before the anticipated expiry date if regulatory or other concerns arise.

The authority demands that the licence holder explicitly warns potential customers that the firm may cease to operate on or before a specific date.

GUIDELINE No 5
KNOWLEDGE-ENHANCING TOOLS

Related fintech products: All

1 Overview

The arrival to the financial sector of multiple products, services and business models supported by recent technological innovations has created an important challenge to financial authorities unfamiliar with the underlying technologies and uncertain about the impact these innovations may have on their ability to perform their duties adequately.

This knowledge gap has been recognised by supervisors in several jurisdictions and this has led to the development of new approaches to increase their understanding on how these new fintech products work, how they interact with traditional financial services and how these products and their novel providers alter the way risks are created and channelled in the financial market.

The purpose of this guideline is to equip the reader to systematically evaluate the suitability of the tools most commonly used by financial authorities in jurisdictions with an active fintech ecosystem, taking into account the limitations that the legal framework, the resources available and the financial market development may bring. Also, the financial authority, when deciding on implementing a specific tool, should take into account the general fintech policy, as described in Guideline No 1 and the overall regulatory framework and supervisory stance.

It is important to keep in mind that the actions described in this guideline must be used as tools to increase the authority's knowledge of fintech products and providers, not as strategies to promote fintech adoption in the jurisdiction.

2 Evaluation topics

2.1 Fintech development and knowledge gap

Fintech activity level in the jurisdiction, in terms of the number and diversity of fintech products, as well as the presence of non-traditional providers, is significant. However, the level of information the authority possess is low.

Regulated financial institutions are introducing fintech products based on technologies unfamiliar to the supervisor.

International financial institutions and large non-financial companies, such as mobile network operators, are implementing fintech products in other jurisdictions that may pose an information challenge to the authority when bringing those products into the local financial market.

2.2 Legal framework

There is no law provision nor jurisprudence (in other areas) to allow live testing of new financial products.

Customers protection law provisions' dispute resolution process deters firms from carrying out tests.

2.3 Authority resources

The financial authority lacks enough resources, such as staff with the right skills and time available to top executives within the organisation, to oversee tests.

The onus of the supervisor mandate focuses on fulfilling its regulatory duties, not the promotion of new firms or products.

It is difficult for the authority to determine the balance between the potential benefits of a tool, in terms of better understanding of specific fintech products, and the strain it may place on available resources.

2.4 Reputational risk

There are potential reputational effects from failure if a test goes wrong, even if customers suffer no financial losses.

Customers participating in a test may have a negative reaction when the tested product or service is withdrawn.

Allowing unproven fintech products by firms with no or very short business history to be provided to customers in a market environment may be perceived as a reckless action by the supervisor. In the case of a regulatory sandbox, this perception may be reinforced by the association of the term with a children's playground.

Testing fintech products in a "live" market environment, targeted at financially excluded customers may be negatively perceived by organisations promoting financial inclusion.

2.5 Regulatory and supervisory improvements

The authority deems that greater understanding of fintech products and their enabling technologies may lead to better tailored regulations and appropriate supervision practices.

Regulated financial institutions have a greater willingness to offer the authority more access to detailed aspects of a new product or technology within a sheltered environment, prior to its introduction into the market.

The interaction between the firm testing a fintech product, the supervisor and, if it is the case, the customers, may allow the supervisor to suggest, or demand, changes to the tested fintech product.

2.6 Relevant experience from other authorities

Financial authorities, both within the jurisdiction and from other countries, are able to share results from tests and other tools, including failed tests.

There are supervisors in similar jurisdictions engaging in knowledge-enhancing tools willing to engage in joint exercises.

3 Potential regulatory and supervisory actions

The following options have been selected from initiatives by financial authorities observed in jurisdictions with significant fintech activity. These actions can all be part of an overall knowledge-enhancing strategy by the supervisor depending on the results of the evaluation proposed in the previous subsection. Some of the options are connected with actions explored in Guideline No 1, Guideline No 3 and Guideline No 4.

3.1 Fintech register

The supervisor invites non-regulated fintech providers to voluntarily provide information about their activities, stating explicitly that inclusion in the register must not be seen as an authorisation or official status recognition by the authority. This option is compatible with whatever the results of the evaluation carried out in the preceding section are.

The register should complement the monitoring activities carried out by the supervisor to identify and gather information on fintech activities in the jurisdiction.

The register should be open to both active fintech providers and firms exploring launching fintech products.

The authority will clearly state that inclusion in the register does not endorse a firm or indicate that an authorization has been granted. Firms may not refer to inclusion in the register in their marketing materials or any other document directed to existing or potential users. The supervisor may share the information with other authorities

as part of a fintech cooperation agreement, as described in Guideline No 3.

3.2 Innovation hubs

The financial authority creates a permanent facility and invites regulated financial institutions and non-financial firms to bring enquiries regarding fintech topics, including information on regulatory requirements to bring new fintech products into the market, licensing options and other topics. The authority may also choose to bring issues for discussion with the participants.

This option is suitable for jurisdictions that face legal constraints and other barriers as described in subsections 2.2 and 2.4, while its impact on resources, as described in subsection 2.3, is lower than in other options.

These hubs can be seen as a combination and evolution of the fintech units and the stakeholders' meetings described in Guideline No 1 and can adopt several modalities, including physical meetings, with one or several participants, online engagements or telephone calls. In addition, record-keeping requirements must be established.

Depending on the legal framework and supervisory practices, any guidance provided by the authorities to questions raised by a participant may be deemed binding or not. The financial authority may opt for reporting the results of these queries publicly or within the hub's participants, either as an official policy statement or as a guidance document.

The design, operation and scope of the hub needs to be clearly articulated and terms of reference established to cover purpose, transparency of outcomes, cooperation, etc. The scope differentiation between a hub set up by the authority and those created by other entities should be clear.

Commonly the financial authority designates the head of the fintech unit (if it exists) as the hub coordinator. The coordinator then invites staff with particular skills from within the organisation to participate in the evaluation of specific queries.

Other relevant authorities may be invited to participate in the hub, either permanently or for specific topics. The participation of all relevant competent supervisory authorities (including for consumer protection and data protection) should be mandated to allow for a coordinated approach to the regulatory and supervisory treatment of new or innovative financial activities.

It should be noted that although innovation hubs are usually portrayed as a centralized interface to answer fintech-related questions from the industry, they provide a relatively easy, low-resource intensive and legally feasible tool to acquire detailed information on upcoming fintech products and the firms behind them.

Additionally, the innovation hub need not be restricted to domestic borders and could be a joint or cross-border initiative. For instance, the Bank of International Settlements (BIS) is establishing innovation hubs which, amongst other things, will identify and develop insights into critical trends in technology affecting central banking and serve as a focal point for a network of central bank experts on innovation. Implementation will entail the setting up of hub centres in Basel, Hong Kong and Singapore as part of the initial phase.

3.3 Fintech regulatory accelerator

This option is suitable for authorities that have do not have legal constraints but face significant reputational risk, as described in subsection 2.4, from engaging in live tests.

This tool allows authorities and firms developing fintech products to execute proof-of-concept (PoC) tests on their products or their enabling technologies in a laboratory environment. Moreover, a detailed description of each PoC and assessment of its potential benefits and disadvantages should be openly available. In most cases, this option is compatible with the legal mandate of most financial authorities.

Regulatory accelerators can comprise several types of fintech provider and authority goals:

a) Start-ups and non-financial companies wishing to test if the products being developed have realistic prospects of gaining regulatory approval;
b) Regulated financial institutions exploring new technologies and products;
c) Financial authorities looking to stimulate the development of fintech products that address specific issues, either to overcome deficiencies in existing financial services or to facilitate the authority's operations, a range of products known as RegTech or SupTech.

In a regulatory accelerator, staff from the financial authority bring the expertise and the supervisor's perspective into the discussions and tests within the accelerator. The authority promoting a regulatory accelerator may provide financial resources to firms participating, particularly in the case of start-ups developing solutions sought by the authority.

Tests within an accelerator do involve neither customers nor real world transactions, therefore there are no regulatory requirements for non-regulated firms to participate. An exception to this limitation is limited testing among the staff of the provider.

3.4 Regulatory forbearance

The financial authority decides to authorise fintech product providers even though they do not satisfy all the regulatory requirements, if allowed by the legal framework. This option requires a positive result from the evaluation of the legal framework, as described in subsection 2.2 and the risk assessment of subsection 2.4.

The justification for regulatory forbearance is to allow specific new fintech products, considered potentially beneficial for the economy, to be introduced into the market when potential providers are not likely to immediately satisfy every standard requirement to obtain a financial services license.

The regulatory requirements that can be relaxed or omitted are the following:

a) Minimum capital: A lower initial capital amount and capital-to-assets ratio, commensurate with the expected risk profile of the firm;
b) Liquidity: Lower liquidity ratios reflecting the specific sources of funding of the firm;
c) Ownership: Fewer independent shareholders and/or higher (or no) limits for a single shareholder stake. This is particularly suited for large non-financial companies already providing a fintech product, which the authority wants to keep in the market, but provided by a separate financial services subsidiary. This is a similar case to local subsidiaries of foreign banks.

Other prudential and non-prudential requirements, such as management fitness and shareholders' suitability to engage in financial services or source-of-funds checks, must not be omitted or relaxed.

This approach is best suited to a case-by-case analysis, rather than a general authorisation policy. Eligible firms will usually be established, well capitalised non-financial companies willing to enter the financial services market. If applicable, the supervisor will apply the standard rules regarding acceptable jurisdiction of origin.

The authority uses discretionary powers explicitly granted in the legal framework, and it requires the imposition of restrictions in the activities of the firms benefiting from forbearance, such as a cap in the number of customers, maximum amounts per customer and other risk-mitigating limits.

These restrictions are in place while the firm does not comply with the exempted requirements. The authorisation, therefore, specifies the timeframe to fully comply with those requirements.

To promote a gradual convergence of the firms benefiting from forbearance of the usual requirements, the

authorisation is subject to a time schedule for gradually reaching full compliance with regulations, matched by a corresponding easing of the restrictions initially imposed.

It is expected that once the firm enjoying forbearance shows that it is commercially viable, it will be able to attract new investors and thence the relaxation of capital requirements will cease to be necessary.

If the authorised firm fails to achieve full compliance by the deadline or misses a goalpost in the schedule, the authority starts a winding down procedure, according to a pre-set process established in the original authorisation. The terms of the licence must also give the authority to cancel the authorisation at any time before its end date, if it detects deviation from the original terms, breaches to the restrictions imposed or the firm infringes other general regulatory or legal provisions.

In case the legal framework does not grant the authority to offer regulatory forbearance, an alternative mechanism to reach the same goal would be to propose the necessary legal reform to create a special, time-limited, fintech licence incorporating the same elements previously described, along the options considered in Guideline No 4 - 3.2.

The supervisor must ensure that it has the necessary staff to closely monitor the performance of the firm and to collect information on the relevant fintech product.

3.5 Regulatory sandboxes

This option requires that the authority is allowed by law, according to the evaluation of subsection 2.2, to engage in this type of test. Also, the authority must be satisfied that it has the required resources available, as described in subsection 2.3, and that the potential overall benefits (subsection 2.5) outweigh potential reputational risks (subsection 2.4).

The supervisor creates a special program allowing firms interested in bringing new fintech products into the financial market to start providing those products to real customers in market conditions, subject to certain restrictions. The main goal is to allow new fintech products to be introduced into the market under a controlled environment.

Although the regulatory sandbox is a scheme open to all interested, the supervisor retains the final decision on whether or not an applicant is granted permission to participate. The supervisor must evaluate each application on the basis of:

a) Expected benefits for customers;
b) How it may increase financial market efficiency and competition;
c) Whether the fintech product to be tested is a genuine innovation;
d) Whether the participant faces evident unnecessary burdens to bringing the fintech product to market;
e) Whether the fintech product has reached the development stage;
f) Whether the proposal includes appropriate safeguards to protect clients' funds in case the applicant fails during the test;
g) Whether the participant has designed an effective customer claims handling process;
h) Whether the applicant holds a financial licence or satisfies all the requirements for obtaining one.

The last criterion may be satisfied either with respect to a standard financial licence or a specific licence tailored for sandbox participants, as described in Guideline No 4 - 3.2. A joint venture by a regulated financial institution and a non-financial company satisfies this criterion as well.

The specific conditions of the regulatory sandbox will depend on the specific fintech product in consideration, but will include at least the following specifications:

a) Time limit: The test must take place over a period long enough to evaluate its characteristics under different market conditions, but should not last longer than one year;

a) Termination conditions: Before reaching the time limit, the authority may end the test if it considers that the fintech product has already failed to reach its intended goals or if it is evident that unexpected risks have appeared;
b) Exiting from a successful test: At the end of a successful test, the participant must be in a position to apply for a regular financial services licence with reasonable prospects of success. In no circumstances can the testing period be extended. If the participant is not able to successfully apply for a licence, it must wind down the business.
c) Winding down: The regulatory sandbox terms must describe the process of winding down the operations, in the case of failed tests, and early termination by the authority or if the participant cannot get a regular licence. The process must ensure that all customer funds, including interest if applicable, are returned and other liabilities are adequately paid. It is worth noting that provisions may differ if an incumbent institution is the one responsible for the fintech product.
d) Test customers: Given the heightened risks inherent to a test, targeted customers must be able to understand the risks involved in the test and should not depend on the funds committed to the tested fintech product for day-to-day expenses. If feasible, in retail product tests customers must satisfy the standard local definition of sophisticated investors. Whenever possible, customers should be selected from the participant's staff.
e) Caps and aggregated limits: For each test the authority will set a limit to the number of customers using the tested fintech product, a cap on the amount accepted from each customer and, optionally a maximum total aggregated amount handled by the participant that is lower than the product of the first two limits.

The authority must take into account that it is committing a significant level of resources by operating a regulatory sandbox. The greater the number and diversity of firms participating simultaneously, the larger the number of staff involved in running the tests and the time the supervisor's top executives must devote to keep abreast of developments. A cost recovery scheme paid by applicants could be considered by the authority, depending on its general fintech strategy.

Careful consideration must be taken when designing the safeguards demanded from participants to address any financial losses and other potentially harmful incidents to customers, as well as threats to the stability of the financial system in case the test fails or if unexpected events arise. In particular, the regulatory sandbox must contemplate the following before and during the test:

a) Participants' management and key personnel understand laws and regulations governing their conduct;
b) Participants engage in appropriate risk management;
c) Participants have sufficient financial resources to sustain operations during the test even if revenue projections fail to materialise;
d) Participants have contracted appropriate insurance policies to cover accidents and internal fraud;
e) Participants are bound to the same data privacy and cybersecurity regulations of traditional financial institutions;
f) Tests involving wholesale transactions among financial institutions must be subject to aggregate amount caps evaluated continuously.

The authority ensures that the regulatory sandbox is not being used to create an uneven playing field in financial markets, either by forcing fintech start-ups to team up with incumbent financial institutions due to the financial burden associated to the tests, or large non-financial companies combining sandbox tests' regulatory benefits, large (non-financial) customer base and financial strength to leapfrog other potential competitors or small regulated financial institutions.

The authority pays careful consideration to how to interpret regulatory sandbox test results, as they may be skewed by several factors. First, the public may be reluctant to engage

with a firm during a test. Secondly, incumbent financial institutions may be unwilling to provide the necessary financial services to the participants, either because of a cautionary stance to mitigate risks or to avoid helping potential competitors. Third, the lack of standardization inherent to a test environment may result in fintech products that are successful in tests but that fail when migrating to full market conditions. Finally, tests may fail to measure whether a fintech product brings cost reduction benefits. This is particularly relevant in small jurisdictions where the market size does not allow for substantial economies of scale promised by technological innovations.

3.6 Joint knowledge gap reduction exercises

From the evaluation of subsection 2.6 it may be possible to identify likely candidates to engage in joint knowledge gap reduction exercises.

In this case, the financial authority motivates counterparts in other jurisdictions to jointly implement any of the tools described in this section by combining resources to make it feasible to conduct such tests, in turns, in each jurisdiction. Cross-border exercises could be an option to consider, however they will demand greater analysis of their legal implications.

The jurisdictions involved must use the same legal systems and have compatible financial legal and regulatory frameworks. Also, their financial systems must have a high degree of similarity, including in fintech activity.

These exercises could be facilitated if coordinated by a regional financial authority's organisation or an economic integration body. It will be helpful to frame this collaboration within the cooperation frameworks described in Guideline No 3.

GUIDELINE No 6
PRUDENTIAL REGULATIONS CONCERNING TECHNOLOGY

Related fintech products: All

1 Overview

The arrival of fintech can be seen as one aspect of financial services' increasing reliance on technological solutions. The digitalisation of financial activities has been a gradual process, accelerated in the last few years by the pressures on financial institutions to become more efficient and meet the demands of customers who expect the same level of speed and convenience they get from other service providers.

Regulators have long recognized that financial institutions need to adapt their risk management frameworks to cope with emerging new risks, with ever-larger financial impacts arising at faster speeds and resulting in severe reputational costs.

This guideline will focus on risks related to fintech products as well as general technological issues specifically relevant to fintech product providers.

2 Evaluation topics

2.1 Traditional financial institutions' reliance on fintech products

Traditional financial institutions are introducing fintech products into their core processes, either by developing these products in-house, contracting the services of a non-financial firm or acquiring firms.

Traditional financial institutions deliver products and services to their customers, and their provision has been supplied via contracts with external unregulated non-financial independent or subsidiary fintech firms.

Non-financial fintech firms act as originators of financial products (for instance, loans and deposits) that are then sold to regulated financial institutions.

Traditional financial institutions incorporate data collected and analysed by third parties using fintech products into processes critical for identifying and measuring risks.

Financial institutions have entered into commercial partnerships with large non-financial companies to give access to the payment system to fintech products provided by the latter to their customers.

Most financial institutions have only one or a few providers of fintech products.

Financial institutions, individually or associated, are exploring the incorporation of new fintech products in wholesale systemwide transactional platforms.

2.2 Adoption of digital services by customers

A significant proportion of financial service customers have adopted digital channels and products.

Traditional financial institutions are reducing their branches' footprint.

Financial institutions incentivise customers to engage through digital channels via fees and shorter opening hours at branches.

2.3 Fintech-specific technology risks

Fintech providers may bring products into the market that are new, developed in-house, based in unproven or very recent technologies and with few comparable experiences. These characteristics may increase the probability that the underlying technologies do not work as they should.

Fintech providers may tend to rely almost completely on digital storage for their customers' data. Moreover, their business models rely on external data storage, network connections and data processing, usually provided by third parties that may also be using recent technologies, increasing the risks of security breaches, losing access to computational services and communications services.

There are scarce historical data in fintech activities to feed risk models, including comparable benchmarks of operational risk incidents, leading to misjudgments in technology risks.

Fintech products may suffer from algorithmic determinism, where complex financial decisions are entirely left to the results of a 'black-box' computer program. Incorrect or biased parameters, or failing to take new information into account may produce unwanted results with likely increased risks, if those results are not scrutinized by humans.

2.4 Operational risk management at fintech providers

Fintech providers that began as small start-ups are experiencing a phase of rapid growth, unaccompanied by a corresponding strengthening of their risk management processes.

Technological arrangements such as data communication, cloud computing, cybersecurity defences, contingency mechanisms, recovery plans and staff level and skills may not keep pace with the challenges brought by the ever-increasing size of the fintech firm's operations.

Technological risk mitigation procedures and tools may not be implemented as rapidly as they should.

Insurance cover for the firm's technological risks may not be available as insurance companies may not be able to price a premium due to scarce or non-existent data.

3 Potential regulatory and supervisory actions

3.1 Evaluate current information technology (IT) regulations in place

The authority should ensure that its IT regulations adequately cover the new technologies being introduced by fintech in the financial market, their emerging risks and increased reliance on technology to deliver financial services.

The authority must ensure that the following areas have been updated to cover fintech developments:

a) Governance of enterprise IT;
b) Business continuity management;
c) IT service management;
d) Outsourcing, including cloud computing;
e) Cybersecurity management;
f) Information security management and;
g) Development and acquisition of applications.

3.2 Requiring a financial institution to evaluate operational risks before introducing new fintech products

In the risk management framework, the supervisor will expect financial institutions, both traditional and fintech-oriented, to carefully analyse the risks brought by every new fintech product. This evaluation has long been considered an essential piece of a sound operational risk management framework to comply with international standards, such as the Principles issued by the Basel Committee on Banking Supervision.[79] In the context of fintech activities, nevertheless, it is important to consider that the information required to assess the inherent risks of a new fintech product, the changes it may bring to the operational risk profile of the financial institution and the corresponding

79 BCBS. Principles for the Sound Management of Operational Risk. June 2011.

mitigation techniques are more difficult to identify, as the evaluators lack relevant data or precedents.

Therefore, it is convenient to incorporate into the evaluation process the following activities, at a minimum:

a) Analyse available results of tests or proof of concepts. If not available, explore possible ways to obtain information of the likely behaviour of the fintech product and the underlying technology in lab conditions (for example, tests among staff).
b) Scrutinize how the fintech product operates, with the participation of staff not involved in the development of the product, if that is the case.
c) Explore the interaction with other processes within the institution and external parties and their readiness to operate with the new fintech product in terms of speed and volume of transactions.
d) Compare the potential revenue-generating or cost-savings benefit against the highest estimated financial losses in case of an adverse event.
e) Evaluate the impact on the current IT architecture if uptake of the fintech product exceeds expectations.

This action should be considered along with that described in Guideline No 2 - 3.8.

3.3 Incorporate the lack of alternative fintech providers into business continuity plans

As some fintech products may be provided by a single external provider, business continuity plans must take into consideration this limitation.

Financial institutions must explore alternative measures, such as temporarily suspending the provision of the affected fintech product, offering replacement options to affected customers or contemplating developing a temporary substitute version of the affected products in-house as a last-resource backup.

It is important that business continuity plans are tested regularly.

The supervisor monitors whether a single large technology firm becomes the dominant player in providing key market infrastructure services to financial service providers, either traditional financial institutions or fintech firms. The supervisor must ensure that regulated firms have credible alternative providers.

3.4 Demand access from third-party fintech providers to evaluate their operational risk management

In addition to the BCBS recommendations on outsourcing technology process, the regulation should include, in the case of fintech products, that a financial institution satisfy itself that the provider's operational risk management processes are comparable to the levels expected from a regulated financial institution.

An independent audit firm should annually review the third party's IT service management. The audit should be in accordance with the International Standard on Assurance Engagements 3402,[80] issued by the International Auditing and Assurance Standard Board (IAASB).

The supervisor, in exercising its duties, should have access to the fintech provider to assess the conformity of its risk management processes to the required standards. This capacity must be expressly contemplated in the relevant contract.

3.5 Define fintech-specific operational risk management provisions

The operational risk management regulations should include the following considerations in the case of fintech product providers:

a) Operational risk assessment procedures must keep up with any increase in size, complexity or diversification of the firm's operations.

80 IAASB. Assurance Reports on Control at a Service Organization. June 2011.

b) Contingency mechanisms and recovery plans must be regularly updated to take into account developments in the range of fintech products offered, customer base, number of transactions processed and other quantitative and qualitative dimensions.
c) The firm must monitor the market for new, suitable and better mitigation tools, and periodically update the existing tools accordingly.

3.6 Cybersecurity defence readiness assessment and remedies

The supervisor informs firms that rely exclusively on digital solutions to interact with customers and store and process data that they must have in place proportionate cybersecurity defence measures.

To verify their readiness to withstand attacks through digital channels, the firms must engage in penetration exercises, carried out by verifiable independent companies[81] on a yearly basis.

The firm, in turn, must require evidence of similar exercises and their results from its technological service suppliers. The supervisor should be able to access those results.

The firms must demonstrate that they have addressed any weakness reported promptly and in line with its severity.

An effective whistle-blowing process could complement these risk mitigation tools.

81 There are a variety of accreditation schemes. The authority usually does not prescribe a specific certification.

The firm must be able to reimburse customers for any financial losses suffered as a result of cyberattacks facilitated by weaknesses in the firm's defences.

3.7 Fintech firms and traditional financial institutions implementing fintech products must demonstrate they fully understand their products' logic

The supervisor expects firms to provide convincing evidence that:

a) The top management understand how their products work.
b) The firm has carried out extensive tests simulating how the fintech product works using a formal test procedure.
c) The firm has tested their systems with different sets of data, including stress testing.
d) Test results are filed for independent review.
e) The board of directors has received detailed information about the characteristics of the new fintech product being introduced and the results of the tests.
f) The firm has a process to update its systems to reflect changes driven by data gathered from usage of its fintech products.
g) The fintech product's underlying algorithms do not result in biased or erroneous decisions.

These requirements should be extended to other financial institutions if they introduce fintech products indirectly as distributors.

GUIDELINE No 7
PRUDENTIAL REGULATION AND SUPERVISION PRACTICES FOR MANAGEMENT FITNESS, CORPORATE GOVERNANCE, INTERNAL CONTROLS, INTERNAL AUDIT AND EXTERNAL AUDIT IN A FINTECH ENVIRONMENT

Related fintech products: All

1 Overview

As part of the evaluation of potential modifications to the regulatory framework to address challenges brought by fintech, it is important to consider policies and procedures that may be left untouched during the revision process.

Financial risks usually differ by line of business – for instance, consumer vs. corporate lending, local vs. cross-border payments – and not by technology. Therefore, a regulated financial institution, whether fintech or not, should have senior officials with the expertise to manage those risks.

Likewise, operational risks related to the use of technology in finance can arise within traditional financial institutions, not only in fintech-oriented providers.

Consumers of financial services, when placing their assets with regulated financial service providers, expect that their senior officials have been vetted by the authority to ensure they have the highest standards of honesty, integrity, suitability and reputation.

Financial authorities, as recommended by the Financial Stability Board,[82] should aim to reduce gaps and inconsistencies in corporate governance-related requirements or standards. This goal is consistent with a proportional approach, based on the ownership structure, geographical presence and stage of development of financial institutions.

The main objectives of an internal control framework, namely, to mitigate risks to acceptable levels and to support sound decision making, are equally required in every regulated financial institution, with varying degrees of complexity concomitant to the financial institution's size, range of services and operating environment. Therefore, fintech firms shouldn't be expected to have a different internal control framework than traditional financial institutions with the same characteristics mentioned before.

Technological innovations in financial services have had a significant impact on how internal auditors perform their jobs. Technologies have created challenges in auditing business processes that are mostly digital and/or automated, in many cases without standards specifically explaining how to do so.

However, those challenges are present in all financial institutions, with varying degrees of intensity and impact depending on the level of reliance on technological processes. Fintech firms are undoubtedly heavy users of technology in their processes, but so are traditional financial institutions.

Fintech activity has gradually moved away from a niche sector populated by small start-up firms to an ecosystem where traditional financial institutions and large non-financial companies are also present.

Emerging small fintech firms are increasingly engaging in partnerships with incumbent financial institutions, either as providers of specific fintech products or as customers for wholesale banking services. In parallel, in order to remain competitive, small fintech firms are actively seeking equity funding to expand operations and to satisfy capital requirements so as to become regulated. These trends imply

82 Financial Stability Board. Thematic Review on Corporate Governance. April 2017.

that small fintech firms must request an external auditor to check their financial records, compliance with regulatory requirements and strength of their internal controls.

This guideline presents elements to evaluate whether specific areas of regulation should be applied equally to fintech and traditional financial services, or adaptation is merited to reflect distinct characteristics of fintech products.

2 Evaluation topics

2.1 Management competence and fitness criteria

Regulations state that management must show competence and suitable skills according to the functions assigned.

Fitness criteria, based on honesty and financial soundness, apply equally to all financial activities involving handling money from customers.

2.2 Corporate governance

Fintech firms are attracting outside investors and even becoming listed companies.

Fintech firms in some instances have an expanded set of stakeholders, such as organisations promoting financial inclusion.

The governance framework, such as the role of the board, conflict of interest policies, codes of ethics, transparency and shareholders' rights, allows adaptations proportional to the size and range of stakeholders.

2.3 Internal controls and audit environments

Regulations require internal control systems and structures proportional to the complexity and the risk profile of the regulated institutions.

Fintech firms are increasingly becoming regulated institutions, either as a strategic decision by the firms or as a direction by the authorities.

External investors expect fintech firms to have internal controls matching their activities and size.

Users of external audits —banks, investors and supervisors— are more comfortable with financial reports following standards applied in financial services.

3 Potential regulatory and supervisory actions

3.1 Apply the same regulation on these areas

The financial authority considers that there are no compelling reasons to adapt regulation on management fitness, corporate governance, internal controls, internal audit and external audit to accommodate fintech products providers' particular characteristics.

The regulator may take, if it is pertinent, a graduated approach to the specific provisions of these regulations, based on the principle of proportionality and taking into account the size, complexity and reliance on technology of the regulated institutions.

The authority may also consider that the generally applied regulations need updating to recognize the increasing use of technological innovations in financial services.

3.2 Design fintech-specific regulations on these areas

Having evaluated the elements in the previous section, the regulator may well conclude that some specific components of the regulations, in the areas discussed in this guideline, do indeed require adaptation to take into account the characteristics of fintech product providers.

In this scenario, the regulator should ensure that this divergent approach neither results in regulatory gaps nor is interpreted as a preference by the authority in favour of either incumbent or innovative financial service providers.

GUIDELINE No 8
NON-PRUDENTIAL REGULATION: FINTECH AND AML/CFT

Related fintech products: All

1 Overview

Like traditional financial services, fintech activities are exposed to the risk of being used to legitimize capital coming from illicit activities or to channel funds to finance terrorist organizations. However, specific features of fintech products, such as remote access to financial services and almost instantaneous execution of fund transfers, create unprecedented challenges for the implementation of robust AML/CFT controls.

At the same time, the same technological innovations underpinning fintech products offer potential advantages when implementing AML/CFT mitigation measures in both traditional and fintech financial activities.

This twofold perspective on fintech has been acknowledged by both the Basel Committee on Banking Supervision (BCBS)[83] and the Financial Action Taskforce (FATF). The BCBS has adapted its guidelines regarding AML/CFT risk management[84] to include the challenges and opportunities arising from fintech activities. The FATF launched a global forum focused on fintech and AML/CFT, with the explicit goal of supporting "responsible financial innovation in line with (…) FATF Standards, and (…) to explore the opportunities that new financial and regulatory technologies may present for improving the effective implementation of AML/CFT measures."[85]

An important aspect of this subject is the possibility that traditional financial institutions refuse or withdraw access to their services to fintech-oriented firms, citing concerns regarding AML/CFT compliance. This policy, known as de-risking, may become a significant barrier of entry for new competitors and can have detrimental effects on financial inclusion efforts. Therefore, creating an AML/CFT regulatory framework for fintech activities, paired with appropriate supervisory practices, may reduce genuine apprehension among traditional financial institutions.

Finally, fintech products based on or using cryptoassets present special challenges to current AML/CFT frameworks. FTAF recently issued two documents on cryptoassets, strengthening its standards to clarify the application of anti-money laundering and counter-terrorist financing requirements on cryptoassets and their providers and setting out more detailed implementation requirements for their effective regulation and supervision.[86]

This guideline presents the main issues that authorities should consider when developing their regulatory and supervisory approaches to AML/CFT risk management in a fintech environment. Also, several courses of action are suggested, taking into account the BCBS and FATF recommendations on this area.

83 BCBS. Sound Practices - Implications of Fintech Developments for Banks and Bank Supervisors. February 2018.
84 BCBS. Guidelines - Sound Management of Risks Related to Money Laundering and Financing of Terrorism. June 2017.
85 FATF. Fintech and RegTech Initiative Statement. November 2017.
86 FTAF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. June 2019 and FTAF. Public Statement on Virtual Assets and Related Providers. June 2019.

2 Evaluation topics

2.1 Digital client onboarding and "Know Your Customer"(KYC) processes

Financial institutions are enrolling new customers remotely through digital channels relying on information provided by the customer for identification.

There is no national identification system, or the existing scheme is not suitable for digital checks.

There are financial service providers with no or a limited physical presence which rely on non-face-to-face due diligence.

Fintech providers are oriented towards financially excluded customers.

The jurisdiction has a financial inclusion strategy that encourages financial service providers to use special customer due diligence processes.

Financial institutions using digital channels to enrol new clients are using KYC processes relying on identification verification carried out by third parties (such as MNOs or agents).

Financial institutions are implementing client identification and/or KYC technological solutions based on new procedures and data.

2.2 Cross-border transactions

Financial institutions are introducing fintech products aimed at facilitating, speeding and expanding the range of jurisdictions their customers can make transfers to or receive them from.

There are new providers of international money transfers using fintech products.

Fintech products are being introduced in the jurisdiction that allows international money transfers completed wholly outside the traditional currency exchange systems (such as cryptoasset trading platforms).

2.3 Cash-cryptoasset transactions

There are cryptoasset "exchanges" that allow users to trade cryptoassets for cash in the jurisdiction.

Trade in cryptoassets takes place at commercial venues.

Information on parties engaged in cash-cryptoasset transactions is unreliable or below the requirements of AML/CFT regulations.

Caps or limits on these cash-cryptoasset transactions are inexistent or unenforceable.

2.4 Potential for technology-based AML/CFT compliance solutions

Financial institutions are facing rising costs of complying with AML/CFT regulations.

There are conceivable synergies between government digital initiatives and technological compliance solutions (for instance, national electronic identity schemes).

Non-financial companies with a great number of financially excluded customers have developed client identity verification systems.

2.5 Financial regulations allow simplified risk-based KYC

The regulations allow financial service providers to offer customer deposit or payment accounts with simplified KYC requirements, subject to volume caps according to a tiered structure of bank accounts.

Fintech products targeted at retail customers, in particular the financially excluded, fit within this scheme with few modifications to the regulations.

2.6 Fintech providers face challenges in fulfilling their AML/CFT

Firms developing around payment and financial intermediation fintech products are experiencing a rapid rate of growth in the jurisdiction.

Risk management systems and procedures, including staff skills and level, in new fintech firms do not keep pace with the increase in the level and complexity of AML/CFT risks.

There are fintech products involving two or more connected firms, each with a varying degree of AML/CFT preparedness or compliance requirements.

It is not clear in these chains which firm is responsible for overall AML/CFT compliance.

3 Potential regulatory and supervisory actions

In addition to the recommendations issued by the BCBS and the FATF, the financial authority following the evaluation results may opt for one or more of the following actions:

3.1 Ensure that AML/CFT regulations are applied consistently in fintech activities

The financial authority, in coordination with other authorities, examines fintech products and their providers and identifies those that fall within its regulatory AML/CFT perimeter and those that must be regulated and supervised by other relevant authorities.

In the case of a fintech product that has several firms involved in its provision, when carrying out that evaluation the financial authority should consider which firm maintains the relationship with customers, and particularly which firm receives and return funds to customers. Similar to traditional financial institutions, a nominated AML/CFT Compliance Officer should be designated with accountability for AML compliance.

The financial authority must be vigilant that all fintech products and providers have been evaluated and that all are subject to AML/CFT obligations and control, according to the nature of their activities.

The financial authority adopts a proportional approach to AML/CFT regulations to fintech activities, on par to the approach to traditional financial activities. In particular, simplified KYC requirements and tiered account structures should be allowed under equal conditions, where applicable, to fintech providers.

3.2 Demand additional measures for digital onboarding KYC processes

If as a result of the evaluation of subsection 2.1 the authority finds that digital onboarding is commonly used by financial institutions, including fintech firms, it changes the regulation to require that whenever a financial institution opens an account for the first time to a customer not physically present for identification purpose, the institution must take a set of extra measures to compensate for any increased risks associated with those customers. These measures should aim to ensure that the customer exists, and the person or company has been correctly identified, and may include the following:

a) Verify the customer's identity using a suitable database, preferably the national identity system database, if available.
b) Further corroborate the identity based on information not previously used for verification, held at reliable public or private sources, such as driver's licence issuers, electoral registers, utility companies.
c) If possible, arrange for the customer to transfer funds from a named account held at another financial institution.
a) Use audio-visual real-time communication for accounts not subject to amount or usage limits. During this video interview, still photos of the customer and of the appropriate identity documents should be taken. These interviews must be recorded and stored by the financial institution and/or fintech firm.
b) Check on the consistency of the location information as provided by the customer with that obtained from the remote connection (IP address or similar).

3.3 Promote fintech-powered compliance solutions

If the authority finds, after considering the elements presented in subsection 2.4, that there is a compelling case for promoting wider adoption of technologically powered AML/CFT compliance solutions, it proceeds to state its willingness to consider technologically-based AML/CFT regulatory compliance tools (RegTech).

The financial authority seeks to facilitate the deployment of RegTech that requires private data sharing between regulated financial institutions and third-party providers, by reaching exemptions to the general data privacy limitations from the relevant authority. In any case, customers must retain the right to explicitly opt in to any data sharing arrangement.

The regulation recognises the equivalence of these AML/CFT risk mitigation tools with those based on traditional procedures.

3.4 Bring cryptoasset trading platforms into the AML/CFT regulatory perimeter

If, from the evaluation carried out in subsection 2.3 it is clear that there are cryptoasset activities in the jurisdiction, the financial authority, if legally viable, or assisted by another relevant authority, enforces compliance with AML/CFT regulation by firms providing cryptoasset-fiat money trading platforms.

According to the results of the risk evaluation, the relevant authority (financial or not) may decide to include transactions involving cryptoassets alone.

The financial regulation discourages the uses of anonymization techniques in cryptoasset-fiat money trading platforms (such as tumblers and mixers[87]).

3.5 Follow the evolution of AML/CFT risk management controls in new fintech providers

The financial authority demands that new fintech providers prepare and submit for assessment plans to keep AML/CFT risk management controls in tune with their expected growth path, introduction of new products and expansion to new market segments or locations.

The plan must anticipate staff number and training demands, development of reporting and other compliance obligations and the capacity of the board and the top management to keep pace with increasing time commitments.

The financial burden of the expected enhancements should be in line with the projected revenue growth.

87 These are services offered to "mix identifiable (alternatively known as 'tainted') cryptocurrency funds, with untainted pools of funds, so as to obfuscate the trail behind the cryptocurrencies." Chohan, U. The Cryptocurrency Tumblers: Risks, Legality and Oversight. Discussion Paper. November 2017.

PRODUCT-SPECIFIC GUIDELINES

In this chapter, regulatory and supervisory topics specific to different sets of fintech products are examined. The evaluation topics and potential responses by the financial authority for each category of fintech products is analysed in individual guidelines.

Each guideline indicates at the beginning the relevant fintech products, using the denominations and identifiers from the general catalogue of fintech products, services and business models. The list of the selected fintech products and their description is in Chapter IV. The structure of the guidelines is the same as those in Chapter II.

Although these guidelines can be treated independently, references are made to issues addressed in the guidelines of Chapter II.

GUIDELINE No 9
FINANCIAL INTERMEDIATION-LIKE FINTECH PRODUCTS

Related fintech products

FTP-01 Loans in balance to consumers
FTP-02 Loans in balance to businesses
FTP-03 P2P loans - consumers
FTP-04 P2B loans - business
FTP-08 Credit risk evaluation using artificial intelligence
FTP-09 Alternative credit ratings
FTP-75 Crowdfunding - real estate
FTP-76 Crowdfunding - capital

1 Overview

Among the wide variety of fintech products, those that resemble or share the most functionalities with traditional financial intermediation – deposits and loans or investments – have attracted the greatest attention. Financial authorities are seeing useful innovations in these products that have the potential to enhance competition in financial markets while reaching segments inadequately served by traditional financial services.

Conversely, in most cases these products have emerged unregulated, reproducing in some cases the same problems that decades of regulatory and supervisory efforts have stamped out from financial markets, such as insider lending or trading, unfair credit practices and opaque information. Moreover, in most cases customers of these fintech products do not enjoy the benefits of financial consumer protection frameworks and deposit guarantee schemes. There are also concerns regarding the lack of proper AML/CFT systems.

This guideline provides the main elements that should be considered when evaluating regulatory and supervisory actions regarding these products, drawn from developments in the last few years by financial authorities in jurisdiction with active fintech ecosystems.

2 Evaluation topics

2.1 Financial market structure

The financial market is characterised by low level of competition, expressed in market dominance by few players. As a consequence, the interest rate spread is larger than desired.

There are market segments underserved by traditional financial institutions.

2.2 Fintech lending and deposit product landscape

Fintech product providers are mostly operating unregulated.

Lack of regulatory certainty limits fintech providers' ability to grow and gain market share.

There have been failures among P2P and crowdfunding providers and exit mechanisms proved to be inadequate,

investors incurred losses or borrowers experienced funding shortfalls.

One or two platforms dominate the market (P2P and crowdfunding).

Platforms tend to focus their lending/investing activity in one economic sector.

Large traditional financial institutions are customers of lending platforms.

2.3 Risk management issues

There are no secondary markets for these products, or they are illiquid.

Lenders do not differentiate between borrowers according to risk of default.

Individuals and companies obtaining loans from P2P platforms have no alternative lender in case the current lender collapses or leaves the market.

P2P platforms lack adequate mitigation tools for maturity mismatch.

Platforms do not retain exposure to intermediated assets.[88]

2.4 Informational asymmetries

P2P and crowdfunding platforms do not satisfactorily reveal credit and liquidity risks to their customers.

P2P and crowdfunding platforms advertise unrealistic and unsubstantiated financial returns for their products.

P2P and crowdfunding platforms do not disclose conflicts of interest.

2.5 Customers financial needs assessment

Crowdfunding platforms do not evaluate their products' suitability for retail customers.

Crowdfunding platforms do not assess potential customers' financial literacy or understanding of the risks involved in investing.

Potential customers are not explicitly warned that the value of their investment can go down or even disappear completely.

2.6 Alternative credit ratings

Providers of fintech credit ratings do not reveal the source of the data used for grading potential lending customers.

Users of alternative credit ratings, including financial institutions, do not fully understand the methodology or the consistency of the data underpinning the ratings.

Customers cannot access the data held by alternative credit rating providers.

Alternative credit rating providers do not provide recourse to customers.

3 Potential regulatory and supervisory actions

3.1 Include P2P and crowdfunding platforms in regulatory perimeter

Financial authorities, either based on interpretations of what qualifies as financial intermediation or by promoting legislative action, bring these fintech products into their regulatory perimeter.

P2P and loans in balance products, as well as credit rating services should fall within the banking regulation, whereas crowdfunding platforms are deemed capital market intermediaries. In the latter case, platforms should comply with rules over disclosure of financial conditions, handling of

88 Traditional reporting requirements are usually linked to the balance sheet, this makes it difficult to track funds intermediated by platforms even if the latter were inside the regulatory perimeter.

client money, requirements that investors must have investment experience and the platform's conflict of interest and risk management.

In this case, it is relevant for authorities to think about whether customer funds should be protected by a deposit guarantee scheme. Platforms at this point have no access to public safety nets, such as central bank emergency liquidity.

3.2 Adapt regulations to recognize the characteristics of these fintech products

The financial authority adapts the regulations to reflect the level of risks of these activities in order to avoid discouraging providers and creating barriers to entry.

Providers must assess customers' understanding of the risk involved and ensure that the funds committed are not required for regular expenses.

In this regard, regulators could impose market restrictions similar to the FCA that would limit direct financial promotions to investors who:

a) are certified or self-certify as sophisticated investors;
b) are certified as high-net-worth investors;
c) confirm before receiving a specific promotion that they will receive regulated investment advice or investment management services from an authorised person; or
d) certify that they will not invest more than 10% of their net investible portfolio in P2P agreements".[89]

P2P platforms must not be allowed to transform maturities; therefore, customers should be informed that funds will only be returned when the corresponding loans mature.

Loan size and maturity must be limited in line with the targeted market segment.

89 https://www.fca.org.uk/publication/consultation/cp18-20.pdf

The P2P provider must retain a set proportion of each originated loan in its balance to align its incentives with its customers'. The proportion must be the same for every loan. To avoid conflicts of interest, the provider must get the same financial terms as the investors from these loans.

Rules on loan loss provisioning are adapted to reflect the distribution of credit risks between the platforms and the customers.

3.3 Ensure fair treatment of retail customers

The supervisor monitors the terms and conditions offered to retail investing customers by P2P and crowdfunding platforms, to identify if traditional financial institutions and other large institutional investors are receiving preferential treatment in the following areas:

a) Interest rates paid by the same borrower;
b) Credit risk information;
c) Earlier redemption policies;
d) Access to secondary markets.

The supervisor checks if platforms are being used by traditional financial institutions to dump high-risk, rejected or close-to-default borrowers.

The supervisor sets a requirement for platforms to develop and make public their conflict of interest policy, including disclosure on transactions by the platform's owners and management as investors.

The supervisor expects platforms receiving funding from traditional financial institutions and other large institutional investors to have contingency plans to protect borrowers in case of a sudden withdrawal of those large customers.

In case the platform arranges a secondary market, the supervisor must monitor whether access and conditions are equal for all investors in a platform.

3.4 Exit policy

P2P and crowdfunding platforms should be required by the regulations to have a written resolution plan, which must include the following:

a) critical process flows, calculations, operational procedures (including all elements outside the platform, as outsourced service providers);
b) hosting arrangements;
c) data backup storage location and credentials for access;
d) arrangements to transfer their operations to other providers;
e) payment and bank systems.

These plans must be updated annually and submitted to the supervisor.

Contracts and other documents supporting the operations must allow their transfer to other platforms, under the same conditions for both investors and borrowers.

Investors must be informed that they stand to lose money in the case of a platform failure, if there is any assets shortfall after allocating the failed platform's capital and accumulated funds provision.

Platforms receiving operations from a failed platform can only accept fully funded operations.

3.5 Bring alternative credit ratings providers into the regulatory perimeter

From the evaluation of subsection 2.6 the authority concludes that there is a compelling case to bring providers of alternative credit ratings into line with traditional firms. The financial authority interprets that the provision of alternative credit rating is a service similar to traditional rating agencies, and thus providers are subject to the same regulation.

Extend the same requirements to alternative credit ratings providers in the areas of scoring models methodology transparency, customers' access to their own data and recourse to correct errors as set for traditional rating agencies.

GUIDELINE No 10
PAYMENTS AND MONEY STORAGE FINTECH PRODUCTS

Related fintech products

FTP-17 Automated savings from user accounts to a new account
FTP-18 Automated savings in social networks from user accounts to a P2P platform
FTP-21 Digital wallets on mobile devices
FTP-22 Virtual prepaid cards
FTP-24 Mobile payments
FTP-25 Mobile payments direct cooperation bank - mobile network operator
FTP-26 Mobile payments - Direct billing to mobile phone account
FTP-29 API credit cards payments
FTP-32 Multi-channel POS
FTP-33 Payments gateway

1 Overview

As the first category of fintech products to be introduced into the financial markets, products that provide payment services and money storage have long attracted the attention of financial authorities. Thus, regulations and supervisory practices are more developed for these products than for other categories of fintech activities.

An important feature in some of these products is that they not only play a role in payments, but also can be used to store money. The line that separates money storage products from deposit bank accounts, from a user's perspective, is vague.

More recently, new fintech products have emerged, building on the initial payment and money storage products, extending their functionality and the range of linked financial services. In particular, this guide addresses services that automatically make money transfers from a user's bank account to another financial service provider, based on an analysis of his/her spending behaviour and income patterns.

Another feature is many of these products' reliance on mobile networks and devices. It is not surprising then, that telecommunications regulators and MNO trade bodies have played an important role in shaping best practices and identifying specific risks.

It is important to highlight that non-financial companies with a large customer base, such as Big Tech, MNOs and online shopping platforms, choose fintech payment services as their first step in financial markets.

Finally, some products in this category have shown a crucial relevance in promoting financial inclusion, generating other public and private sector stakeholders' attention to the development of a conducive regulatory framework.

This guideline will focus on issues where regulations and supervisory practices are still evolving, adopting the perspective of the financial authorities, with a goal of both promoting beneficial innovations and reducing risks.

2 Evaluation topics

2.1 Regulatory fragmentation

Similar services (such as mobile payments) are provided by different categories of firms: financial institutions, MNOs, large technological firms and fintech firms.

Different types of providers are regulated and supervised by different authorities or are unregulated.

Unregulated providers operate joint ventures with regulated firms.

Technological innovation and functionality extensions are creating or widening existing regulatory gaps.

Payment service providers exempt from regulation on the basis of 'limited network exclusion' (mainly those used only for purchases in a single retail store chain or public transport system) are extending their functionality.

MNOs are allowing users to pay for other firms' goods and services with money stored in their accounts (either as e-money or as prepaid services) or directly billed to their accounts.

2.2 Fintech providers' interconnection with traditional financial institutions

Fintech firms can access real-time payment systems, often after a reduction or elimination of minimum amounts and fees for transactions in systems operated by central banks.

Fintech products offered by large non-financial providers include push and pull arrangements with financial institutions.

Large fintech providers placing customer funds in bank accounts/trust have become significant depositors who, in turn, may cause an impact on liquidity risk management at financial institutions.

2.3 Restrictions on money stored and customers' fair treatment

Most current regulations forbid digital wallet and other fintech payment providers to pay interest on stored funds, including funds pending settlement.

Firms offering these services are allowed to earn interest on customers' funds. Determining who should benefit from this is an issue that could be addressed.

Fintech firms offering these services cater to users without access to traditional financial institutions.

2.4 Regulatory treatment of fintech firms not holding client funds

Fintech firms act as payment initiation services, accessing a user's payment account to initiate the transfer of funds on their behalf.

Fintech firms exclusively provide account information services, such as financial account aggregators.

Fintech firms provide financial advice based on consumer financial data.

2.5 Risk management framework at fintech providers of these products

Liquidity management at financial institutions and funds kept by large fintech firms.

Diversification of customers funds' custodial arrangements.

Separation of funds raised as money storage from the payment firms' assets

Impact on customer funds in the event of a custodial financial institution insolvency.

Cybersecurity, fraud and AML/CFT risks management in fintech products involving several providers in the value chain.

3 Potential regulatory and supervisory actions

3.1 Recognise diversity of providers while minimizing regulatory gaps

Deriving from the results of the evaluation of the elements in subsection 2.1, the financial authority, acting in coordination with other relevant authorities, harmonizes the

regulatory framework by type of service, considering the function and characteristics of each service.

For large, potentially systemic non-financial providers, the financial authority, with assistance from other relevant authorities, encourages setting up dedicated subsidiaries subject to financial market regulations. This must be a mandatory action if the fintech products become more complex or transcend simple payment or money storage functions.

3.2 Compatible customer protection schemes

Each relevant authority must set customer protection procedures that are consistent across market segments.

The regulations set clear dispute resolution mechanisms, with access available through the same channels used by customers that make use of such services.

Customers must be able to close their accounts through the same channels used to enrol in the service.

3.3 Reduce differentiated regulatory treatment of funds stored in payment and money storage fintech products

Fintech providers of these services should seek to have funds placed at financial institutions in custodial agreements earn interest.

This income must be explicitly recognized as belonging to their customers and distributed, net of reasonable administrative expenses, accordingly.

In case of a custodial financial institution failure, funds held in custodial agreements must be treated as belonging to the fintech providers' customers for deposits guaranty limits, if applicable.

3.4 Adjust risk management regulations

The regulatory framework for liquidity risk management at financial institutions should recognise the emergence of large fintech payment product providers as a source of liquidity risk.

At the same time, rules on how these large fintech providers invest their clients' funds must ensure that they are spread among several financial institutions and that there are limits on exposure to a single financial institution. These regulations should be coordinated across relevant authorities to ensure their consistency.

Financial institutions should ensure that third parties have obtained express permission from their customers to access data and initiate transfer or payments.

Financial institutions must satisfy themselves that these fintech providers have robust cybersecurity, data protection and AML/CFT risk management systems in place.

3.5 Promote competition in financial markets by enabling financial advice fintech products

The financial authority develops a regulatory framework that enables fintech products that allow financial customers to compare, analyse and act on their current financial arrangements, based on their income and spending patterns, to gather relevant data from financial institutions.

The regulation ensures that the data exchange and the execution of connected financial transactions by providers of these fintech products is carried out in a safe manner, with customers retaining ultimate control of these transactions.

These providers should register with the financial authority, but would not become regulated financial institutions, but technical service providers. However, these firms must agree to comply with technical specifications set in regulations. The register is public but clearly states that the firms included are not financial institutions. Financial institutions are responsible to ensure adherence to these specifications by firms accessing their systems.

The regulation forbids the use of the data gathered by these providers for other purposes than those explicitly

stated on their websites and in other public commercial documents.

The regulations should encourage financial service users to change providers easily and with reduced costs.

3.6 Regulations provide a clear roadmap for providers of evolving fintech products

The regulations take a proportional approach to these fintech products, allowing non-financial firms engaged in single and non-complex payment and money storage fintech products to remain within their original regulatory perimeter, if there is adequate coordination among relevant authorities and rules on the provision of those services are consistently applied.

The financial authorities inform non-financial firms that are exploring expanding their portfolio of fintech products, extending the functionality of those currently provided or achieving a specific volume of transactions or number of clients, that they have to become a regulated financial institution or set up a regulated subsidiary.

Large non-financial fintech providers operating in partnership with unrelated regulated financial institutions should also be subject to mandatory conversion to or divestment from a subsidiary if the activity they channel through the regulated institution becomes a significant proportion of their overall business.

3.7 Exit policy

The authority makes sure that all fintech payment service providers are bound to a predefined resolution procedure, ensuring that customer funds are promptly reimbursed to their bank accounts or transferred to another provider.

Special consideration must be taken with transactions in transit, preferably by stipulating that these operations settle as originally planned.

These procedures must be coordinated between the financial supervisor and the central bank, wherever they are separate entities.

GUIDELINE No 11
CRYPTOASSET PRODUCTS

Related fintech products

FTP-23 Prepaid cards based on cryptoassets
FTP-37 Cryptoasset payments integration
FTP-39 Inter-bank trading platform based on cryptoassets
FTP-41 Foreign exchange trading using cryptoassets
FTP-44 Cryptoasset digital wallet
FTP-45 Digital wallet combining legal tender and cryptoassets
FTP-46 Off-line cryptoasset digital wallet
FTP-47 Cryptoasset physical exchanges
FTP-48 Cryptoasset online exchanges
FTP-50 Cryptoasset ATMs

1 Overview

Among fintech products, those using cryptoassets remain the most controversial, in no small part due to the initially poorly understood nature of cryptoassets. As a result, financial authorities have taken starkly divergent approaches, even within the same jurisdiction.

Another factor that has led to conflicting positions is the potential that both financial institutions and authorities see in cryptoassets' underlying technologies: blockchain and distributed ledger technology (DLT).

Only 10 years since their first incarnation as alternatives to central bank-issued currencies, cryptoassets are permeating every corner of financial markets and have evolved from a small niche product favoured by those wanting to operate outside the formal financial system, into a technological innovation explored by central banks themselves.

Financial authorities' responses range from a complete ban on any cryptoasset-related transaction to an official endorsement of such activities.

Cryptoassets' features as decentralised products, unbound by national boundaries and accessible through multiple channels, make it almost impossible to enforce a complete ban. Most jurisdictions that have adopted a favourable policy towards cryptoassets have a tradition of providing a high degree of privacy to foreign users of their financial services.

At this point in time, cryptoassets can potentially bring both harm and benefits to financial markets and their users. How to strike a balance in one or another direction is still a work in progress.

It is safe to say that the initial goal of the creators of the first cryptoasset, Bitcoin, has failed. Conceived initially as a system to "allow online payments to be sent directly from one party to another without going through a financial institution,"[90] its main attraction nowadays is as a speculative financial asset, sought for potential capital gains rather than for making payments online.

Cryptoassets' use as a means of payment remains severely limited, their role as store of value has been eroded as their price in fiat currencies has fluctuated markedly in the last few years and holders have suffered significant losses due to fraud and other operational events.

90 Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009.

There is no evidence of prices of goods or services set in any cryptoasset. Thus, cryptoassets do not fulfil the criteria of a currency. This is why there is now a consensus among authorities and some in the private sector to use the term cryptoasset instead of cryptocurrency.

Making transactions using cryptoassets does not necessarily guarantee anonymity for the parties involved. This is particularly true whenever those involved in this type of transaction transform their cryptoassets into fiat currencies. There are techniques that reduce the likelihood of identifying those trading cryptoassets. However, those techniques were developed, and are still being used, in transactions involving regular money.

Most, but not all, cryptoassets require decentralised systems, DLTs, to record ownership, involving a certain degree of consensus among participants to validate any transfer of ownership. The ownership registry is usually contained in a digital file, the blockchain, encrypted in such a way that any alteration can be detected by solely looking at the file history.

Blockchain files are usually publicly available for inspection and participation in DLTs is mostly open to all interested. Not all cryptoassets use open access DLTs to validate transactions, make blockchain files available for public scrutiny or use blockchain as a registry. Each technology, blockchain and DLT can be used in financial and non-financial applications not involving cryptoassets.

Although in its early days, Bitcoin and other first-generation cryptoassets were chosen by criminals to carry out illegal transactions, steps taken by authorities have reduced their attractiveness for eluding controls.

Gaps in regulations, authorities' lack of expertise in identifying users in encrypted transactions and lack of constraints in cross-border transactions remain powerful incentivel for moneylaundering through cryptoassets. Buying and selling cryptoassets with cash remains a possibility in some jurisdictions, facilitated by some innovative products and the use of retail agents. However, there are operational limits to these transactions. Inherent weaknesses in cryptoasset exchanges have attracted cybercriminals' attention, resulting in successful raids on customer assets, both in fiat currencies and cryptoassets.

The speculative price bubble experienced by cryptoassets in late 2017 prompted fraudsters to launch "initial coin offerings," enticing users to invest in what was seen as a "sure bet" on capital appreciation, without checking the business case behind the new cryptoassets.

Use of cryptoassets as an alternative for foreign exchange has shown they can provide faster and cheaper service than traditional services.

Currency exchange transactions using cryptoassets' DLT or equivalent decentralised settlement schemes can even substantially reduce inherent credit risks in the prevailing system based on third-party counterparts.

Cryptoasset transactions most likely begin and end with accounts held at traditional financial institutions. Therefore, weaknesses in the cryptoasset ecosystem can have an impact on financial institutions. Cost-reduction targets are driving financial institutions to develop wholesale transactional platforms based on cryptoassets' functionality.

Cryptoasset exchanges are increasingly seeking closer links with traditional financial institutions, to facilitate their clients' access to fiat currency, for example, by issuing debit cards backed by international franchises.

It is very difficult to define in which jurisdiction a cryptoasset is based, as most cryptoassets lack an issuer, in the sense that there is no firm or individual for whom cryptoassets are a liability. At the same time, cryptoassets are particularly suited to cross-border transactions.

This guideline focuses on the main challenges financial authorities face from cryptoasset-related products, services

and business models, providing a stylised catalogue of topics for evaluation. Then, a set of potential regulatory and supervisory actions is presented. It is not the goal of this guide to suggest a specific course of action, as each authority must define its cryptoasset policy based on the legal framework, the financial market structure and the degree of penetration of these products in their jurisdiction.

2 Evaluation topics

2.1 Firms dealing with cryptoassets in the jurisdiction

Firms involved in cryptoasset transactions in the jurisdiction have a non-financial background.

Governance, internal controls, cybersecurity preparedness and AML/CFT systems may be weak or even absent in those firms.

Unclear regulatory framework and contradictory policy statements have deterred firms from seeking regulatory approval.

Local firms involved in cryptoassets lack a clear business case, beyond pursuing growth. This, in turn, limits their capabilities to fund robust control systems.

2.2 Cross-border challenges

Users in the jurisdiction are able to carry out transactions in cryptoassets with foreign firms remotely.

There are several routes to channel local currency to or from non-local cryptoasset exchanges.

Divergent approaches towards cryptoassets among authorities make the use of existing cooperation and information exchange MOUs difficult.

2.3 DLT and blockchain developments by financial institutions

Regulated financial institutions are exploring financial applications of the technologies underlying cryptoassets, either locally or by their parent companies abroad.

3 Potential regulatory and supervisory actions

3.1 Coordinated public authorities' approach to cryptoasset activities

The financial authorities state a single interpretation of cryptoassets and define the allocation of firms providing related services to the relevant market segment.

Financial authorities set a coordination task force with the objective of:

a) Analysing the cryptoasset ecosystem in the jurisdiction.
b) Carrying out joint risk assessments on cryptoasset activities.
c) Harmonising regulations applied to cryptoasset activities.

The financial authorities seek cooperation from authorities from the jurisdiction of origin of cryptoasset exchange platforms remotely offering access to users in their jurisdiction.

3.2 Reduce negative impacts of cryptoassets while allowing innovations

The authorities warn users of the dangers of engaging in transactions with unregulated providers of cryptoasset-based products.

In parallel, the financial authority issues regulations bringing points of contact between the cryptoasset ecosystem and the financial system, fundamentally cryptoasset exchange platforms, under the regulatory framework, either as payment services providers or as securities intermediaries, in at least the following areas:

a) AML/CFT regulations, in particular KYC and suspicious activity reporting obligations;
b) Customer protection scheme;[91]
c) Cybersecurity preparedness;
d) Internal controlQs and governance.

Additionally, cryptoassets used for payment purposes would generally fall under the monetary authority, while digital tokens used for investment purposes would be under the remit of the securities regulator. A determination is needed on classification to a single exclusive class, which is often problematic given simultaneous functioning across multiple categories.

3.3 Supervisory approach towards cryptoassets' use and support by financial institutions

Request financial institutions to provide detailed information of cryptoassets, blockchain or DLT-based products prior to their launch.

Request financial institutions providing financial services to cryptoasset exchange platforms to carry out enhanced due diligence on the platforms' readiness to comply with AML/CFT and cybersecurity controls.

Request financial institutions' support in identifying potential points of cryptoasset-cash exchange, such as retail stores and independent cryptoasset ATMs. Furthermore, authorities should consider establishing a mechanism to verify conversion and exchange rates and publishing prices and the methodology used to determine those prices in a bid to boost transparency.

3.4 Proactively monitor developments in this area

The financial supervisor tasks a unit to follow up on developments in cryptoassets and their underlying technologies. In particular, the following trends should be closely observed:

a) Implementation of systems-based cryptoassets and related technologies by financial institutions, at home or by their group elsewhere.
b) Developments of cryptoasset products by non-financial firms with a large existing customer base in the jurisdiction.
c) Emerging applications based on cryptoassets and related technologies with applications in regulation and supervision.

91 There are still considerations to be resolved regarding the recourse of the customer against the wallet or exchange operator, as well as provision of disclosures to consumers related to service fees or charges associated with crypto transactions.

GUIDELINE No 12
NEW BUSINESS MODELS

Related fintech products

FTP-12 Virtual banking
FTP-13 Mobile phone banking
FTP-14 Mobile network operator (MNO) and financial institution convergence
FTP-20 Social network integration - payments - finance – retail
FTP-38 Banking information integration platform
FTP-40 Foreign exchange operations P2P/B2B
FTP-56 Banking as a platform (BaaS)

1 Overview

Thanks to recent technological innovations, there has been a marked shift in financial service provisions towards remote and digitally based interactions between financial institutions and their clients.

This evolution has allowed for the emergence of new business models that harness the possibilities brought by widespread access to data networks, either from homes and business premises or via mobile phones and other devices.

These new business models are being implemented by existing financial institutions, either directly or through dedicated subsidiaries, by non-financial firms with an existing large customer base and by new players, taking advantage of reduced entry barriers into financial markets.

In some cases, the fintech product provider does not seek to offer financial services but to enable financial institutions, whether new or existing ones, to digitise their activities by 'subscribing' to their services, in what is known as "banking as a service" (BaaS).

This evolution brings new challenges to the regulatory frameworks and to traditional supervision practices, as some of the expected features of financial activities are absent or radically changed. There is also a potential trend, already seen in China, for some of these alternative business models surpassing their traditional peers in terms of asset size and number of customers.

In parallel, there is some evidence[92] that customers seem to prefer remote interaction with their banks, through digital channels, instead of dealing with human staff at branches. Also, in some jurisdictions trust in new players, especially Big Tech firms, is higher than in traditional financial institutions. Strikingly, users in the largest financial markets of Latin America show both a preference for technologically mediated interaction in financial services and the largest decline of trust in traditional financial services.[93]

This guideline provides a structured way to assess how these trends impact the regulatory framework and the financial authority's capacity to effectively supervise the emerging financial institutions. It does not address general

92 EY. Global Fintech Adoption Index 2019. June 2019.
93 Edelman. Trust Barometer: Financial Services 2018. March 2018.

issues covered in other guidelines, such as technology (Guideline No 6) or AML/CFT (Guideline No 8).

2 Evaluation topics

2.1 The digitalisation of financial service provision

a) Branch networks are losing their relevance as financial institutions and their customers migrate to digital channels to execute most financial transactions.
b) Customer are getting the same quality or better level of service in remote interactions.
c) Traditional financial institutions face obstacles in keeping a consistent level of quality in digital channels due to issues with legacy systems.
d) Financial service providers opting for a purely digital infrastructure are able to offer better financial terms to their customers.
e) However, growth in market share by purely digital financial institutions has been limited and, in some cases, they have failed to reach a sustainable size.
f) Corporate clients, in particular, seem reluctant to switch their business to virtual banks.

2.2 Collaboration between financial institutions and non-financial firms

a) Non-financial firms, MNOs in particular, are keener to engage in collaborative agreements with traditional financial services, wherein the non-financial firm acts as an originator and distribution channel for the financial institution.
b) The role of the non-financial firm in these agreements, vis-à-vis regulatory frameworks and supervision of financial activities is not always clear.
c) There are some concerns this trend may lead to a "disintermediated" or "utility" bank, which could make the regulated financial institutions highly reliant on its relationship with the non-financial firm.[94]
d) A financial institution opting for BaaS as a solution to digitise its services could become entirely dependent on a single, mostly unregulated non-financial firm in what could become its most significant distribution channel.

2.3 Non-financial firms with large customer bases becoming financial service providers

a) New business models powered by fintech products are allowing non-financial firms, originally providers of online shopping, communication or social media services (Big Tech) to become significant new players on their own in financial markets.
b) Past experiences in the jurisdiction – such as retail stores offering credit cards - are not comparable, as on this occasion, the potential to capture a significant market share and to compete effectively with traditional financial institutions is much greater.
c) Big Tech can potentially amass a significant client base, intermediating funds between shoppers and the businesses selling goods and services in their platforms.
d) Big Tech firms may be able to cross-subsidise financial products with revenue from other activities.
e) Big Tech firms' access to and capacity to analyse large amounts of data may provide a competitive advantage over financial institutions.
f) Big Tech, potential competitors of financial institutions, are also the main providers of basic services to digitised financial institutions, such as cloud services, digital advertising and communications.

3 Potential regulatory and supervisory actions

3.1 Adapt regulations to recognise specific features of virtual banks

The results of the evaluation of the elements presented in subsection 2.1 should inform whether the financial authority should develop a specific regulatory framework for virtual banks, emphasising the need for robust business

94 BCBS. Sound Practices - Implications of Fintech Developments for Banks and Bank Supervisors. February 2018.

continuity and recovery plans, cybersecurity measures and board members with strong technological skills.

Virtual banks should be required to provide a physical location where customers may bring claims or queries, in addition to any existing digital channel.

Virtual banks are required to promote safe digital practices among their clients. To this end they should make available related literature and information as well as other tools to mitigate cybersecurity risks among their users.

3.2 Impact on traditional financial institutions strategic risk assessments

The supervisor expects traditional financial institutions to evaluate challenges brought by new digital competitors in their strategic risk assessments.

This evaluation should include investments required to maintain a competitive presence in digital channels.

Financial institutions must also analyse the impact on their bottom line of aggressive competitive pricing by virtual banks in products suited for digital delivery.

A careful evaluation of the reliance on core digital services provided by competitors should be included in any assessment.

3.3 Supervisory approach to BaaS providers

The supervisor expects financial institutions outsourcing all or most of the digital presence to a BaaS provider to have carried out a detailed analysis of the decision's impact on their risk profile.

Outsourcing activities does not discharge the board of directors and senior management of their responsibilities. Hence, it may be considered necessary to create internal interaction structures with the outsourced companies, which allow the managers to exercise responsibility in an appropriate way.

The financial institution must ensure that the selected provider has credible and updated business continuity and recovery plans.

The contract should include service level agreements that adequately compensate the financial institution for losses incurred if the services fail or do not reach the agreed-upon quality standards.

The financial institution's own business continuity and recovery plans must include alternate providers, time to switch and costs likely to be incurred.

3.4 Supervisory approach to financial services provided by large non-financial firms

The authority should evaluate the likelihood of large non-financial firms becoming significant players in the financial market, according to the elements evaluated in subsections 2.2 and 2.3.

When a large non-financial company makes an application to become a licensed financial service provider, the authority considers the potential size and market share it can attain given its existing customer base in non-financial activities. Also, as detailed in Guideline No 4, the applicant must satisfy that its management, board members and key staff have relevant financial expertise in large financial institutions.

Finally, if the applicant firm is also a key provider of essential technological services, the supervisor should consider a corporate structure that ensures there is no negative impact on competition in the financial market.

The financial authority must be satisfied that a large non-financial firm willing to start providing financial services presents a plan that:

a) Involves setting up a separate dedicated subsidiary;
b) Takes a gradual approach;
c) Brings in qualified board members and senior staff;
d) Defines strict boundaries between financial and non-financial activities within the group;
e) Shows that the financial service subsidiary is financially viable on its own;
f) Identifies and addresses potential conflicts of interest from non-financial services provided by the group to other financial institutions;
g) Shows that the financial service subsidiary's use of core technological services provided by other firms within the group are provided in similar commercial terms as to other competitors;
h) Identifies potential data privacy issues within the group;
i) Defines exit policies according to the size and systemic relevance of the financial activities of non-financial companies, including potential impacts on traditional financial institutions and other fintech firms.

GUIDELINE No 13
FINTECH PRODUCTS WITHIN TRADITIONAL FINANCIAL INSTITUTIONS

Related fintech products

FTP-15 Bank account opening on mobile phones
FTP-51 Smart contracts
FTP-52 Intra and inter financial messaging
FTP-53 Multiplatform banking solutions
FTP-54. Use of social network data for financial purposes
FTP-55 Analysis of customer behaviour data
FTP-57 Integration of fintech in banking
FTP-58 Fintech and financial institution connection platforms
FTP-60 User authentication by blockchain / cryptoassets
FTP-64 User voice authentication
FTP-65 Financial users' automated interaction
FTP-66 Digital identification
FTP-67 Use of data from social networks and other sources to identify people and companies
FTP-68 Innovative compliance software
FTP-69 Innovative risk management solutions
FTP-74 Cloud storage based on blockchain

1 Overview

Financial institutions have a long history of implementing technological innovations that, among other drivers, reduce costs or bring competitive advantages. Regarding fintech, the attitude is no different, although this time they are compelled to study and implement these innovations as they may risk losing market share to new players, both small and large.

Although not exclusive to traditional financial institutions, the focus of this guideline is to analyse how specific fintech products are being implemented by these institutions to automate, streamline or digitise existing core processes.

Different techniques, collectively known as artificial intelligence, are being introduced in various core processes: lending, risk management, fraud prevention, trading and customer interactions. Verification and approval of products based on algorithms underlying artificial intelligence require officials with both financial and technological skills and outside the teams responsible for the design.

The decision-making logic processes embedded within these algorithms must remain well understood by top management and board members. To get good results from any artificial intelligence system, the data feed must be accurate, complete and consistent.

For supervisors, evaluating artificial intelligence may require handling data from other sources to execute verification processes. These data sets may require transformation to be useful in verification processes.

The goal when implementing most automated processes is to remove human participation, thus reducing errors attributed to staff. As a consequence, streamlined processes, from data input to execution, run faster. Cost reduction-driven implementation of automated process may omit features to allow internal controls and external examinations, including by supervisors, to be performed with the same detail as manual processes.

The next section discusses relevant areas for assessing the impact of these innovations on financial institutions' risks profiles and how they are supervised. Next, several policy options are described. It should be noted that this guideline does not address regulatory and supervisory practices regarding cybersecurity and the implementation of new fintech products by regulated entities, as those topics are treated in Guideline No 6.

2 Evaluation topics

2.1 Automated processes' risk management

a) Financial institutions in the jurisdiction are increasingly relying on automated analysis of large data sets to make financial decisions.
b) There are no clear procedures in place to ensure the data's accuracy, completeness and consistency.
c) Management does not routinely balance cost reductions and potential financial losses due to flaws in their risk assessment of automated systems, as the losses are difficult to estimate.

2.2 Supervisor capability to effectively understand processes

a) The supervisor observes that due to digitalisation, the amount of relevant data that the banking sector is generating is vastly expanding.
b) Traditional periodic reports, in predefined formats, are no longer suitable for detecting a deteriorating trajectory in time to implement corrective measures.
c) Financial institutions are investing significant amounts in IT systems and/or in outsourced contracts to support these new fintech products.
d) Financial institutions are hiring staff with new artificial intelligence and other quantitative skills to complement their financial teams.
e) The supervisor is not be able to replicate these trends. Deploying IT systems capable of handling the data and computational requirements to carry out their supervisory tasks may be difficult due to budgetary constraints. Suitable skilled staff may be scarce in the jurisdiction and, as usual, better remunerated by regulated entities.
f) The supervisor cannot legally use cloud services to cope with these computational demands, as the providers are outside the jurisdiction.

2.3 Fragmentation of value chains

a) Financial institutions are dividing and outsourcing processes within a financial service or product.
b) New customer acquisition, lending processes, risk management systems, customers transaction processes and contract execution are increasingly handled by different firms, expanding the range of outsourced services.
c) There is a growing concentration risk of a reduced set of providers of these services.
d) The supervisor faces constraints on these resources (staff numbers and skills as well as time) to monitor individual components of these segmented value chains., some even operating beyond the jurisdiction.

2.4 Impact on risks

a) Trading and lending decision-making by artificial intelligence systems used by regulated institutions are being developed by a reduced number of firms, relying on similar algorithms and data sets. This increases systemic risks as flaws in those systems' logic may lead a significant proportion of financial

institutions to execute transactions in the same wrong direction.

b) Usage of off-the-shelf risk management and compliance software by regulated financial institutions may lead to risk assessments that do not capture individual circumstances.
c) Financial institutions are increasingly relying on unregulated external providers, including social networks, to identify new costumers and other KYC processes, increasing reputational and AML/CFT risk exposure.
d) Automated user authentication based on innovation may expose customers and financial institutions to greater cybersecurity risks.

3 Potential regulatory and supervisory actions

3.1 Enhancing supervisor capabilities

The supervisor must:

a) be able to understand the algorithms underpinning artificial intelligence systems;
b) have the data handling and analysis capability to carry out detailed verifications;
c) consider reducing intervals between reports or even move towards real-time reporting.

If the supervisor faces budgetary constraints to achieving these goals, it may consider:

a) requiring financial institutions implementing artificial intelligence systems to provide the supervisors with appropriate training materials and other information;
b) proposing that financial institutions set up a jointly held firm to develop a centralised repository of data relevant to supervision purposes. The firm will process, store and harmonise the data and provide the supervisor with secured access to extract reports and detailed data.

3.2 Adapting supervisory processes and supervised expectations

The supervisor informs financial institutions that it expects board members and top management to be fully aware of emerging and increased risks brought by the fintech considered in this guideline.

The supervisor checks if the board, when approving automated processes, becomes aware of expected outcomes arising from the system and the results of tests verifying these outcomes.

The supervisor verifies that the board has obtained assurances that any underlying algorithm logic complies with regulations.

The supervisor expects than in key core processes, there are human verification measures.

The supervisor obtains evidence that the board takes into account benefits beyond cost reductions when approving automated processes.

3.3 External participants in financial product value chain

The supervisor takes into consideration, when estimating systemic risks, the concentration of key financial automated processes in financial service value chains with a reduced number of external unregulated providers.

The supervisor prompts regulated financial institutions to include access to inspect and evaluate risk management processes in contracts with those providers granting the authority.

The supervisor expects financial institutions to include in their internal risk assessments the impact and mitigation measures of sharing the same external provider of key automated processes in financial services value chain with other financial institutions.

ANNEX 1

SET OF PRODUCTS AND SERVICES FOR WHICH REGULATORY GUIDELINES AND SUPERVISORY PRACTICES WILL BE PROPOSED

LIST OF SELECTED FINTECH PRODUCTS

The following are the fintech products selected to develop the guidelines contained in this document. A detailed description for each is provided, and a number, assigned in an initial fintech product catalogue.[95] Some have been omitted for this document, therefore, there are gaps in the numbering sequence. The products are presented classified by market segments.

Segment: Deposits and lending

The fintech products included in this segment are basically oriented toward offering alternative modalities of money intermediation between individuals or companies with surpluses and those with financing needs, omitting financial institutions as intermediaries. Their place is occupied by unregulated firms (in the region), which are limited, according to the usual description of their services, to facilitating meetings between funding suppliers and seekers.

This means that the intermediary firm does not provide any maturity mismatch service, nor does it assume the credit risk in the transaction. In some cases, information asymmetry is reduced by risk analysis provided by the intermediary firm. However, these cannot be equated to formal credit assessments.

The attractiveness of these modalities is that the gap between the interest rate paid by the recipient and what the contributor gets is much less than the spread between lending and deposit interest rates for individuals and SMEs in the banking market.

However, when the service is provided by firms outside the financial regulatory perimeter, users do not enjoy the usual protections of the traditional financial system, such as deposit guarantee mechanisms, credit risk mitigation tools and rules against self-lending.

Another important group of products included in this segment are those related to individual credit risk ratings, using data and methodologies different from those in traditional financial activities. Providers of these services use data obtained from the interaction of people in social networks, cellular mobile telephony usage and similar activities to derive information elements that allow lenders to evaluate prospective clients' character and ability to pay, even for people who lack financial history.

These services can be useful to expand the universe of people who can be granted credit, depending on how successful the models used are. But at the same time, the use of potential clients' information, often obtained without consent and from third parties unrelated to the financial activity, opens the door to possible actions against the user's fair treatment and improper use of private data. Similarly, in these cases the person does not enjoy the same rights as those who are evaluated by regulated credit bureaus, such as the right to know the information stored, error correction and removal of outdated information from the records.

95 The initial catalogue and the descriptions were extracted from a document prepared in May 2018. Therefore, some references may not be relevant today.

FTP-01. Loans in balance to consumers

This product encompasses companies that offer loans to individuals, without deposit intermediation, but which differ from traditional loan houses in the use of innovative technologies to contact customers, evaluate their applications, distribute funds and manage collection.

In some countries these companies establish alliances with businesses, especially medium and small ones, so that they can offer their customers sales on credit. In others, as in the LAC region, they reproduce existing microfinance schemes (use of agents, targeting the excluded) but make use of technology to channel credits.

The main feature of this fintech product is the use of cellular data networks for transmitting information between the contact points of the credit applicants (shops or credit agents) and the company.

These companies finance the credit activity with their own funds, as well as with resources obtained from investors. Companies retain credit risk on their balance sheets.

FTP-02. Loans in balance to businesses

This product is offered by non-intermediary companies that offer loans to businesses, mainly small establishments that do not have access to traditional banking. They usually use information obtained from business invoicing to make a credit decision, using systems based on artificial intelligence.

The processing and communication with the applicant are usually done remotely, through the Web or through applications on mobile phones or tablets. They also tend to respond to requests more quickly than financial institutions that use traditional credit evaluation schemes.

Unlike FTP-05, the credits are not tied to invoices receivable that the business has, so the applicant can use the resources for expansion of premises, acquisition of machinery, among others.

These companies finance the credit activity with their own funds, as well as with resources obtained from investors. Companies retain credit risk on their balance sheets.

FTP-03. P2P loans - consumers

This fintech product consists of an online platform in which natural persons applying for loans meet investors who offer the funds on previously agreed-upon returns. Investors can be individuals or companies, including financial institutions.

The premise of the product is that the investors deliver the money to the company that manages the platform, and then select specific consumers, who may or may not be identified, allocating portions of the amount invested among these consumers as the investor considers appropriate.

Normally these platforms offer some type of guidance to the investor on the credit risk of the consumers, either offering the rating of a credit bureau or using an internal rating methodology.

In this business model, investors assume the entire credit risk, which is mitigated exclusively by the distribution of their funds among multiple recipients. The investor can establish ranges of terms, credit ratings or other criteria to filter out those considered too risky.

The attraction for investors and customers is that the interest rate tends to be better than what they would obtain in the formal financial system, especially for investors. But this in turn allows the company that operates the platform to set relatively high levels of commissions for the work they do, although always lower than the margins prevailing in financial institutions.

In some countries outside the region, financial institutions have begun to channel their loans through these platforms, as a mechanism to diversify their portfolios and to reach clients that would probably be more expensive to engage with directly.

In the cases identified in the region, there is no clarity on how the funds received from investors are kept pending assignment. This can be important since those applying for credit only receive the funds once the resources allocated by investors reach 100% of the total requested. Hence, cash balances not available to investors could be significant within these platforms' magnitudes.

Another aspect is that, since most of these platforms were created recently, they have not experienced a full economic cycle, nor is the effectiveness of their arrears collection mechanisms clear.

FTP-04. P2B loans - business

These are online platforms where businesses apply for loans and investors offer the funds under previously established terms and interest rates. Investors can be individuals or companies, including financial institutions.

Operating in a similar way to FTP-03, this product is mainly differentiated by the loan applicant, a formally established company or entrepreneur, and by the use of invoices receivable as an element for the evaluation of the applicant's credit risk.

Although the platform operator documents the loan that the business receives as a factoring, investors assume the entire credit risk, without recourse to the document itself.

As in FTP-03, it is not clear how the funds received from investors, committed to applicants, but not yet disbursed, are kept.

Another aspect is that, since most of these platforms are fairly recent, they have not experienced a full economic cycle, nor is the effectiveness of their arrears collection mechanisms clear.

FTP-08. Credit risk evaluation using artificial intelligence

This credit product uses artificial and related technologies to simultaneously analyse unstructured information. Usually the company that has the information and controls the distribution of the loan (which may or may not be a regulated financial institution) allies with a software company that offers the information analysis platform. It then generates, as a result, an indicator that guides the lending decision by the originator. This product is aimed at people who are usually not eligible for credit from traditional financial institutions, either because they do not have a relevant financial trajectory for traditional models or because the amounts requested are not large enough to justify a standard credit evaluation.

The most commonly used distribution channel for this product is shops, which offer their customers financing through the fintech company, usually as part of the sales process in the store (physical or virtual). Therefore, the process of identifying the applicant, collecting the required information and approving the loan must be very quick.

Usually, the lender offers mobile phone apps, both to stores and customers, to request and receive information about the loans. Loan assessment processing and storage of information take place in the cloud.

FTP-09. Alternative credit ratings

These are providers of credit ratings based on information different from that used by credit bureaus, obtained from social networks, the use of mobile phones, web page visits, purchases over the Internet, as well as psychometric data including how the user completes loan application forms. The service is aimed at financial institutions and other credit granting companies that wish to expand their potential customer base or simply outsource part of the consumer credit analysis process.

Fintech firms use artificial intelligence, semantic analysis and cognitive analysis in addition to traditional financial sources to generate a credit rating. This rating is offered to the financial institutions, usually a few minutes after receiving the information and at a low cost.

It should be noted that the criteria and methodology used by these companies are not public. Similarly, the

way in which they obtain individual information is not disclosed publicly.

FTP-12. Virtual bank

This product refers to financial institutions that provide all their banking services through digital channels: web pages, mobile phone applications and direct connections such as APIs and similar. It can be a newly created bank, designed to operate exclusively through these channels, or a traditional financial institution that uses these channels under a different commercial brand.

The use of multiple electronic communication channels allows this type of financial institution to have companies as customers and offer a wider range of products and services, for example, those that require sending large (electronic) documentation.

In some cases, including those identified in the region, the bank operates its own independent ATMs. Similarly, some have a call centre, but one mainly oriented towards solving problems, not carrying out transactions.

FTP-13. Mobile phone banking

This product refers to a financial institution that provides all banking services exclusively through a mobile phone app. Thus, it is a restricted variant of FTP-12.

Due to the exclusive use of the mobile telephony channel, it is mainly oriented to individuals. However, banks using this model are all quite new, which does not allow for a determination as to whether they will eventually look for other distribution channels to serve businesses.

FTP-14. Mobile network operator (MNO) and financial institution convergence

This product refers mainly to the acquisition of a banking licence by a mobile network operator, usually through a subsidiary. In most cases, it has been the natural result of the incursion of the MNO into financial activities, initially through payment instruments, then storage of money in electronic wallets and finally loans.

It should be noted that most MNOs in the region have financial institutions among their shareholders in their countries of origin. This seems to have acted as a barrier to formal incursions into financial products. However, these MNOs offer their subscribers services and products that, if integrated, would be quite similar to standard financial products: prepaid balance transfers between clients, cross-border prepaid balance purchase, allowing users to keep using services with zero prepaid balances, with a penalty payment linked to the period with no balance, and acquisition of goods and services using prepaid balance.

More directly, two MNOs in the Caribbean have taken that step. Orange, an MNO based in France and active in that country's islands in the Caribbean, recently launched Orangebank. Another MNO, Altice, based in the Netherlands and with operations in the Dominican Republic, is in talks to secure a bank licence, according to press reports.

FTP-15. Bank account opening on mobile phones

These are services that allow natural persons to open a new savings account, even if they are not a current client of the financial institution, using a mobile phone and without having to go to a bank branch.

In several countries in the region, as a result of government initiatives to promote financial inclusion, there are basic savings accounts which can be opened with minimal identification requirements, with no fees for the saver, but subject to limits in balances and transactions. These accounts can be easily provided via mobile phones.

In other regions, it has been private companies that are offering this service, associated with financial institutions to attract new clients.

The verification of the identity of a new client can be done using various methods. In the region, we identified two main procedures: verification in the mobile network operator

subscribers' database and image verification, comparing a photo taken with the mobile phone and a photo stored by the national identification authority.

FTP-17. Automated savings from a user's accounts to a new account

This is a service providing the ability to order transactions in the user's bank accounts. Therefore, it requires the user to authorize the service provider to not only access their bank accounts but also to make transfers to deposit or other remunerated accounts in a different institution. The user authorizes the firm through a mobile phone app.

Transfers are made following rules defined by the firm and selected by the user. In addition to transferring periodic fixed amounts, as in financial institutions, these rules can be associated with the user's expenses level, type of expenses incurred, the level of idle resources in non-remunerated accounts, his/her income and expense profile and even compliance with physical effort goals detected by portable micro devices.

This service uses tools derived from artificial intelligence, such as machine learning and semantic analysis to interpret the descriptions offered in the balance sheets of its users' accounts. It also requires connection via API with participating banks.

The remunerated account associated with the service is selected by the firm, without an indication on whether it is segregated from its own accounts.

FTP-18. Automated savings in social networks from user accounts to a P2P platform

These are services that a firm provides to users of social networks, similar to FTP-17, but in this case in the form of automated dialogue software (known as chatbots) inserted into the messaging system of social networks, mainly Facebook, instead of mobile phone apps. In this case, the chatbot, developed by independent firms, has the ability to connect with financial institutions, with the user's authorization, via API.

Like FTP-17, the company that offers the service analyses the information using machine learning to generate transfers from the user's bank accounts to an investor account, opened in the user's name, in a P2P loan platform, such as those described in FTP-03.

Segment: Payments

In this segment, as the name implies, are fintech products linked to intermediation in payments. Within these, those that allow the realisation of small payments, often using a mobile phone, without the use of cash or traditional physical cards (debit or credit), stand out. These include both the products available to the user and the devices, systems and software required by retailers.

This convenience for the user and the retailer nevertheless brings with it a high dependence on the information systems that support the transactions. This could lead the user of these products to suffer financial losses due to the risk associated with operational failures or criminal action.

Products linked to cryptoassets deserve a special mention in this segment. Even though this type of financial asset has a very limited use in payments, its acquisition with legal currency, as well as its eventual sale, poses important challenges for the integrity of the financial system. Likewise, they expose users to counterparty risk, without a clear understanding on the part of the users.

FTP-20. Social network integration - payments - finance - retail

This case refers to a business model in which a conglomerate is created, usually progressively, around a social network or instant messaging service, which then adds a funds transfer and payments service between its users and participating companies.

The vertical integration of the conglomerate can extend, on the one hand, to online retailers and conventional stores, and on the other, to the acquisition or establishment of a regulated financial institution.

This conglomerate has a special significance as it can reach a wide audience, many of whom are just starting a financial relationship. Hence, its ability to identify and distribute products and services, including financial services, using the Internet and mobile telephony, taking advantage of the information it gets in all the segments in which it operates, could give this type of conglomerate greater leverage compared to other fintech start-ups and even traditional financial institutions.

The most relevant case is a payment service developed by Facebook through its two instant messaging services. This case does not reflect a vertical integration as advanced as that observed in China and surrounding countries. However, it cannot be ruled out that this model, as exemplified by firms such as Alibaba and Tencent, extends to other incipient technological conglomerates with presence in the region. Although at the time of preparing this document, Facebook's service only works in the United States and the European Union, we expect it will eventually be launched in other countries, including Latin America and the Caribbean.

FTP-21. Digital wallets on mobile devices

This is a product that allows the user to "store" money in an account associated with a mobile phone. This account can be associated with a SIM identifier, when it is offered by a mobile network operator, or linked to a mobile phone app, when the product is provided by a financial institution or a non-financial company.

Funds transfers between wallet users are channelled through SMS/USSD messages or through data transmission. To add to or withdraw funds from the wallet using cash, as well as to use the stored value to pay for goods and services, requires the participation of retail stores. Usually there is a contract agreement between the store and the MNO, although this is not strictly necessary since non-affiliated stores can do the same transactions, as long as the store owner/manager has a wallet as well. In some countries, transfers to and from accounts in financial institutions are possible as well.

FTP-22. Virtual prepaid cards

In this case, a non-financial company offers through the Internet, including by mobile telephony, the sale of virtual prepaid cards for single or repeated use, in one or several currencies, issued under one of the international credit card networks. There is no credit evaluation and the company that sells the product does not require prior authorization in most jurisdictions.

The card can be issued in the name of the buyer or not. In the former case, the process of customer identification varies between countries, and in many cases the company requires that the initial purchase and subsequent recharges, if allowed, must be paid with bank transfers, in order to avoid AML/CFT regulations.

It should be noted that several suppliers accept payments from web-based electronic wallets, in practice catering to customers anywhere in the world.

FTP-23. Prepaid cards based on cryptoassets

These are prepaid cards, issued in various currencies under one of the international credit card networks which, unlike FTP-22, are physical cards and are acquired and recharged by selling cryptoassets. Companies that offer the product are usually cryptoasset trading platforms (FTP-48) and/or cryptoasset electronic wallet service providers (FTP-44). In several cases, these companies acquire the cards from an intermediary who manages the direct commercial relationship with the credit card network.

It should be noted that since the issuance of prepaid cards, under the schemes of the credit card networks, can take

place in different countries or currencies, and the storage and sale of cryptoassets is also very much an activity that lends itself to being offered remotely, prepaid cards purchased with cryptoassets are available in any country to which the cards can be sent by mail.

Limits on value, identification or not of the card holders and time validity are defined by the credit card networks.

FTP-24. Mobile payments

A mixture of fintech products is included under this denomination. Their main feature is to allow users to pay for purchases using a mobile phone or other mobile device. In some instances, the service allows fund transfers to third parties, charged to the users' bank accounts or credit cards at a financial institution.

The main difference with the electronic wallets described in FTP-21 is that this service does not allow for the storage of money, only for channelling funds in transactions between accounts. This means that it is offered mainly by financial institutions, directly or in association with a company that provides a specific platform, usually a mobile network operator or a mobile phone manufacturing company.

FTP-25. Mobile payments, direct bank - mobile network operator cooperation

This service is a variation on FTP-24, in which the provider is a mobile network operator, associated explicitly or not with one or more financial institutions. In some cases, the MNO is associated with a firm that operates a payments gateway (FTP-33), through which payments are channelled to financial institutions.

FTP-26. Mobile payments - Direct billing to mobile phone account

This service is another method of FTP-24 mobile payment, in which, as in FTP-25, the provider is an MNO. However, in this case, payments made by the user are not reflected as a debit in a financial institution account or credit card. Instead the MNO charges the user, either in a monthly bill or against a prepaid balance.

This method allows individuals without bank accounts to pay for transactions using an electronic means of payment. Its usefulness depends heavily on the coverage of the retail stores and service providers accepting payments through the scheme.

FTP-29. API credit card payments

These are services provided by a company that operates a payments gateway (FTP-33) through a computer code (API) that offers retailers and other firms to integrate a customer payments facility in online stores, including mobile payments, into their own systems. This offers transparency to the buyer and avoids having the retailer handle credit card details. For the buyer, the API appears as one more option to cancel the purchase.

Usually the API provider acts as an intermediary between the customer, the retailer and the credit card issuer. The retailer receives payment from the API provider, while the card issuer charges the buyer's account, and transfer funds to the API provider. The product can also process debits in bank accounts.

FTP-32. Multi-channel POS

This is a combination of a device, software and agreements that integrates all payment methods required by a retailer. into a single solution. The device can be a traditional POS terminal, or an mPOS, with software that includes functionalities and agreements with a payments gateway (FTP-33).

With this product, a retailer can sell through various channels: online, in physical stores or in temporary stores, and accept payments using a range of accepted instruments, including mobile payments (FTP-24), with cards or over the Internet, in addition to cash.

FTP-33. Payments gateway

Also known as payments aggregators or processors, this product refers to a set of services that a firm provides to various participants in commercial transactions. It is usually established as an intermediary between businesses that require payment solutions (acceptance, authorization and processing, through multiple channels, different currencies and countries), and the financial institutions that in the end accept the charges for the transactions.

For financial institutions, this service simplifies the relationship with retailers with low sales volume, that are geographically dispersed and/or are operating without a fixed premise, all of which prevent a traditional merchant-bank relationship.

They are also an essential service provider for other fintech products, such as FTP-25, FTP-29 and-FTP-32, among others.

Their ubiquitous presence, especially in e-commerce and fintech developments, has made payments gateways important players, with a clear tendency towards consolidation. None of the major firms has emerged locally, but most have a commercial presence in the region.

FTP-37. Cryptoasset payments integration

This is a service that allows retailers, both online and conventional stores, to accept as payment the transfer of certain cryptoassets from the buyer's account to the retailer's account. To some extent it is similar to FTP-33, adapted to payments with cryptoassets.

An element that has prevented further expansion of this service, especially in recent months, is the high volatility that, in regular money terms, prices of main cryptoassets are experiencing (and probably related to the fact that cryptoassets have not been adopted as a unit of account for goods and services).

FTP-38. Banking information integration platform

This is a service offered to firms that require access to their users' bank account information. The data provided include the current and available balance, name under which the user's bank account is registered, pending transactions, transaction location and category.

The company that operates the service obtains the information directly from financial institutions and payment processors, usually using an application programming interface (API).

Its clients are mainly companies that offer advisory services and automatic management of personal finances, such as those described in FTP-25, FTP-29 and FTP-32, among others.

FTP-39. Inter-bank trading platform based on cryptoassets

This product is a wholesale transactional platform for currency trading and settlement between financial institutions, using distributed ledger technology (DLT) and a special cryptoasset defined by the firm developing the system for a group of international large banks.

The system, in the testing stage, would allow the settlement to occur directly in the accounts of the participating banks, in real time, without the need for correspondent accounts (nostro) between the participants, nor for central counterparties.

The platform, understood as a network of computers that make up the DLT, is for the exclusive use of the participating financial institutions, which validate changes in the underlying blockchain, as a result of each transaction.

Potentially, the system would allow for trading and settlement in multiple currencies simultaneously, without requiring a chain of bilateral settlements, as is the case today.

FTP-40. Foreign exchange P2P/B2B operations

These are foreign currency exchange transactions for individuals and firms, aimed at matching bilateral flows, setting an equilibrium exchange rate for both parties, usually equal to or close to the relevant interbank exchange rate. The principle behind this product is the same as that of FTP-03 and FTP-04.

The firms that offer this service usually have obtained licences to operate as forex intermediaries. Generally, the service is oriented without distinction to individual and business, varying only in the identity checks required by the anti-money laundering regulations in the jurisdictions where they operate.

The service is provided online, through the Internet and mobile phones. With few exceptions, providers accept clients from most countries, through agreements with local financial institutions, allowing users to send and receive funds through their local payment systems. Hence, the firms' physical establishment is not very relevant to the user.

Some providers offer digital wallets with different currencies as well.

FTP-41. Foreign exchange trading using cryptoassets

Foreign currency exchange for people and businesses, using cryptoassets as an intermediate step. The cryptoasset can be specific to the service or not. The service provider records the transaction first as a cryptoasset sale in the country of the user remitting the funds, paid in local currency with a local bank transfer. Then, it records a second transaction, as a mirror cryptoasset purchase in the recipient's country, with a local bank transfer in that country's currency. The service provider must run a cryptoasset exchange in both countries.

Therefore, the firm can argue that it is not carrying out foreign exchange transactions, just trading cryptoassets. The implicit exchange rate between currencies is equivalent to the current cryptoasset, in the exchange run by the provider, at the moment when the user requests the operation.

FTP-44. Cryptoasset digital wallet

This product is an "account" in which the user keeps the information required to trade cryptoassets. The cryptoassets themselves are stored in a blockchain; a shared file distributed in a public computer network. The wallet then contains the public "addresses" and the private "keys" that the user requires to receive or transfer cryptoassets. To receive a cryptoasset, the user must provide any of the addresses in his wallet. These addresses are created by the user. It is usual to use one for each transaction. The private keys are essential to initiate an instruction to transfer cryptoassets to another person. The transaction is then recorded in the blockchain.

The wallet can be stored in an application on a user's computer or mobile phone, or online. In the latter case, the online wallet service can be provided by dedicated firms, but usually wallets are integrated into the only cryptoassets exchanges systems (FTP-48), when trading cash settlements take place outside the exchanges.

It should be noted that firms providing this service have shown a high vulnerability to attacks from third parties who, by taking control of their internal systems, proceed to steal both users' and the exchange's private keys to transfer ownership of the cryptoassets, causing losses to users. Similar frauds against users have also occurred by exchanges' staff.

A variant of this service that seeks to mitigate the first of the aforementioned risks is the so-called "cold storage" wallet. In this case servers storing the wallets are disconnected from the Internet and other networks. The service provider in this case process transactions requests from users, and connects those servers for short periods of time, mitigating the exposure to external penetration.

Another risk is the default of the counterparty that is delivering money in a transaction, since the settlement does not occur under the delivery versus payment scheme, as is the case of purses that combine money and cryptoassets (FTP-45). This exposes the sellers of cryptoassets to the possibility of transferring property without having received the money or, having received it in the first instance, that the buyer takes advantage of the absence finality in the cash leg and annuls the payment, after obtaining the cryptoasset ownership.

As the cash exchange is not integrated with the trade and changes in the wallet, the service provider's location is irrelevant, and its users can be located in any jurisdiction in which they have access to the Internet without limitation.

FTP-45. Digital wallet combining legal tender and cryptoassets

This product is an account usually maintained in an online cryptoasset exchange (FTP-48) in which the user stores both money and cryptoassets. Although the description resembles the product FTP-21, this account serves mainly to cancel or receive the product of the sale of cryptoassets in the respective platform. This account can be linked to payment transactions, when it is used in combination with products such as FTP-22 (prepaid cards) and FTP-37 (cryptoassets and payments integration), but in itself it is not a payment instrument. The user can also transfer cryptoassets to another account, its own or third-party, inside or outside the platform that offers it.

These platforms face the same risks indicated for FTP-44, except counterparty risk.

It should be noted that this type of service is the most obvious point of contact between all products from the cryptoassets ecosystem and the financial system, so, unlike other products, it allows for their inclusion within the regulatory perimeter. However, the use of payments gateways (FTP-33) and other mechanisms for transferring funds abroad allow residents of a country to open and store money in this type of wallet even in cases where local authorities do not allow the service.

FTP-46. Off-line cryptoasset digital wallet

This is a combination of an electronic storage device and software, allowing the user to store cryptoassets offline, thus avoiding the risks of loss associated with FTP-44. Similar in appearance to a USB memory stick, it also requires a keyboard or other mechanism to interact with the user.

Although an owner of cryptoassets could opt to protect his holdings by writing the addresses and associated private keys on paper, this is not a practical trade.

Thus, this product combines the protection of keeping holdings disconnected from the network with the possibility of occasional trades, for which the wallet is briefly connected to a computer so as to order cryptoasset ownership transfers.

FTP-47. Cryptoasset physical exchanges

This product refers to a service that allows users to buy cryptoassets with cash inside a store's premises. Most commonly, the store provides the ability to complete the cash payment of transactions agreed upon an exchange (FTP-48) that does not have an integrated wallet, such as FTP-44. These transactions do not necessarily have to take place in the business that offers the service.

This type of service is attractive to those interested in acquiring cryptoassets and who do not have bank accounts, computers or mobile phones with the capacity to install apps, or who have little knowledge of how to trade cryptoassets. It should be noted, though, that not many formal commercial establishments openly offer this service.

A variant, which entails additional risks, is to agree to delivery or receipt of cash with the counterpart in person. Another variant that some platforms offer is to cancel

the purchase through commercial networks that accept payments for services.

FTP-48. Cryptoasset online exchanges

This is a service providing a transactional online platform to trade cryptoassets, in exchange for money or other cryptoassets. Most reproduce the characteristics of traditional financial asset transactional platforms:

a) Orders book with specific prices and amounts
b) Lists, sorted by price, of current orders
c) Information on the latest completed trades

A notable difference from other financial markets is that the barriers to create an order (as opposed to just taking one) are quite small, mainly having a minimum amount of the relevant cryptoasset.

Another difference is that the bidder appears identified with a self-selected username when registering on the exchange, essentially operating under anonymity vis-à-vis other traders. However, we could not identify any exchange operating under a blind or semi-blind scheme, as in traditional markets.

Most platforms offer a digital wallet service, combining money balances and cryptoassets (FTP-44), allowing for the settlement of transactions under the delivery-versus-payment scheme.

Those without combined wallets use escrow accounts, whereby the seller, either the order creator or an order taker, releases the blocked cryptoassets when he/she is satisfied with the money settlement leg. Several of these platforms, to mitigate the risk of non-compliance, have developed trader ratings schemes, as well as information on their trading history in a way similar to those existing in online stores.

Exchanges perform a user's identity verification process at the time of registration, but the quality of the process is inconsistent, depending on the jurisdiction.

FTP-50. Cryptoasset ATMs

These are ATMs manufactured by companies, unrelated to regular ATM manufacturers used by financial institutions, specially designed to exchange banknotes and cryptoassets. This product refers to a service provided by a non-financial company (usually a store) by installing one of these devices on its premises, which customers can then use to settle the purchase of cryptoassets, simultaneous or prior. Likewise, customers can withdraw cash by selling cryptoassets.

These ATMs are not connected to banking networks, but rather to one or more cryptoasset exchanges (FTP-48). Usually the business is the owner of the ATM. Its cost is moderate compared to those used by the banks. The ATM operator independently decides which banknotes the ATM will accept and delivers currency, denominations, minimum or maximum amounts, as well as collects fees for the service.

Segment: Infrastructure and market support

This segment includes fintech products developed for processes within regulated financial institutions, or for transactions between them, rather than with general users. In this case, the main driver for these institutions is cost reductions, through the automation of processes and tasks currently performed by staff. There are also products that expand banks' potential market by making it possible to attract customers without setting up branches. Most of these innovations are recent and there is no historical record allowing for an adequate risk assessment, except for technological risk. It should be noted that among these products, several seek to assist compliance with existing regulations, so-called RegTech, which can facilitate the work of the supervisor, as long as the product is properly designed.

FTP-51. Smart contracts

A blockchain technology-based product, it facilitates, ensures, reinforces and executes contracts and agreements. Its main feature is that the consequences of its content,

for example, payments or compensations, among others, are associated with the occurrence of an event that can be verified independently and automatically by the computer system processing the contract.

As the smart contract is written within a blockchain, it allows all participants in the system to verify it at all times. Any modification to the contract requires validation by all participants.

To date, there are few smart contracts incorporated into financial products in the market. One of them is parametric insurance. However, several financial institutions have announced that they are testing them, mostly within the context of inter-bank operations.

Firms specialized in the implementation of smart contracts for use in financial markets generally design the system that writes, verifies and distributes smart contracts, in specific closed computer networks. Hence, the designing firm's association with and control over the product extends beyond its implementation.

FTP-52. Intra and inter financial messaging

This is a closed, secure, encrypted and cloud-based instant messaging service, initially developed for internal use by Goldman Sachs, then expanded to include a group of 14 other financial institutions. The motivation was, on the one hand, a reaction to the access to messages interchanged between traders and analysts from traditional providers of these types of services, especially Bloomberg. At the same time, it was also in response to requirements from supervisors to keep records of all messages exchanged by traders and other staff, to allow executives at financial institutions to monitor staff, in order to ensure that there are no activities contrary to proper conduct, as well as to provide authorities with searchable evidence.

The service has tools for semantic analysis, machine learning and Big Data analytics, allowing risk managers at financial institutions to ensure that their employees do not engage in activities that could lead to sanctions by regulators.

The company that manages the service began to offer the product to companies in other sectors, always under the concept of a closed group.

FTP-53. Multiplatform banking solutions

This refers to a set of solutions, integrating software and in some cases equipment, that allow financial institutions to start or improve the distribution of their products and services through various digital channels, such as banking through the Internet, mobile phones, SMS/USSD messaging, kiosks and social networks.

In this way, the financial institution avoids having to develop or acquire the necessary tools individually, ensuring an adequate integration between all the channels.

FTP-54. Use of social network data for financial purposes

This service, provided by firms specializing in Big Data analytics, artificial intelligence, semantic analysis, among others, offers financial institutions to gather useful information obtained from the interaction of current or potential clients in social networks.

Social networks provide the specialized firms, charging a fee, aggregate and individual data on over a hundred variables. These firms process this data into quantitative information from which they can extract indicators about individuals, such as predisposition to pay loans, consistency of the information submitted in loan applications, clients' events that could induce buying specific financial products, and alerts about changes in employment, personal or family status.

For financial institutions, one of the advantages of this service is that it allows them to make quick decisions, at a lower cost than traditional analysis methods and

usually with greater precision. It is particularly well suited for use in massive and remotely provided products and services.

On the other hand, the unconstrained use of customer data, other than that from credit bureaus, may expose financial institutions to contravene privacy protection regulations.

FTP-55. Analysis of customer behaviour data

This service focuses on interpreting customers' activity in order to determine the best strategies to maximize the commercial relationship, as well as maintaining or improving customer retention to prevent or reduce losses due to default.

Unlike FTP-54, the information comes mainly from the financial institutions' own records. The service provider offers solutions to integrate systems and databases, frequently isolated or incompatible, along with techniques of Big Data analytics, cognitive analysis and machine learning, to interpret and give meaning to the information obtained, in order to generate recommendations for action.

FTP-56. Banking as a platform

This is a concept that covers a range of business models in which a financial institution, holding a licence, opens its services to other financial service providers, usually non-banks, keeping certain central functions for itself, such as current accounts and the connection to the payments system.

In its most extreme meaning, the financial institution becomes a mere platform, open to any provider as long as it meets certain minimum requirements. In this business model it is feasible that two or more providers of the same service or product are present in the platform, the client choosing which one to use specific products or services. In this model, even a competing financial institution could become an external provider in the platform.

These providers mostly connect to the platform through an API, allowing clients of the financial institution to access their services or acquire their products.

In the business model, known as banking as a service (BaaS), the financial institution that manages the platform establishes the criteria that a hopeful provider must meet, and the rules for offering services and products on the platform. This includes net income distribution and risk assignment.

Clearly oriented to new financial institutions, it is also of interest to fintech companies, which in this way achieve a distribution channel for their financial products and services, with the financial institution giving access to facilities beyond their reach. Also, under this model, fintech firms can add experience with a view to their eventual transformation into banks or other types of regulated institutions.

An essential piece in this model is a firm that provides, independently, the tools that allow the platform to function as a single entity vis-à-vis the client, while at the same time putting into practice the restrictions and delimitations set by the operating financial institution.

FTP-57. Integration of fintech in banking

This refers to how products developed by fintech firms are integrated into traditional financial institutions: the acquisition of fintech by the financial institution. While in the past the incorporation of technological innovations in banking occurred mainly through the acquisition or own development of systems, machines or processes, the speed of innovations and the emergence of unexpected ideas has motivated most of the large financial institutions to closely monitor fintech firms, acquiring those considered useful.

In some cases, especially when the innovation may contain reputational or unknown risks, the purchasing financial institution keeps the acquired firm original brand, while, at the same time, it avoids the competition acquiring that fintech firm.

One of the most widely used approaches to ensure that fintech products under development are under close scrutiny is for financial institutions to set up tech incubators and venture capital funds. Also, it allows them to verify the feasibility of fintech products in conditions closest to reality.

FTP-58. Fintech and financial institution connection platforms

This is a service that offers an online platform where fintech firms and financial institutions can meet and explore partnerships. It represents a more open scheme compared to FTP-57, since the platform is usually managed by an independent third party. In some cases, these platforms arise from government initiatives to promote new companies, in which case fintech is just one of several types of start-ups firms aspiring to contact established businesses.

The platform enables testing products under development by fintech firms in restricted spaces (sandboxes), with technical assistance from financial institutions and others, such as authorities.

It is usually oriented to firms with fintech products at an initial development stage, requiring interaction and technical assistance from businesses, rather than financial support. Joining these platforms is seen by fintech firms as a step towards an eventual invitation to a tech incubator or business accelerator.

FTP-60. User authentication by blockchain/cryptoassets

This is a service that aims at establishing a mechanism to digitally identify users of banking services, with cryptoassets or, more broadly, blockchains.

This service would work in a closed distributed ledger network (DLT) in which each participating financial institution creates and manages identity modules of its clients, including the pertinent documentation. Then they can authorize other participants to access these modules to verify new clients and for KYC processes. For further validation, it is contemplated that national authorities could provide identity confirmations.

The unique feature of the scheme is that only those with demonstrated need to carry checks will have access to the data, removing concerns about privacy and data security that may arise when sharing identity details.

FTP-64. User voice authentication

This is a product specialized in recognizing the identity of customers who use voice communication channels with financial institutions. It is a key piece of other products such as FTP-65, as it allows to authorize a user to perform transactions in their bank accounts, without the need to interact with an employee from the financial institution. It replaces authorization schemes based on secret codes introduced through the telephone keypad or the supply of personal information to human operators, which have been shown to have serious vulnerabilities.

The implementation of this product has been limited, partly because it also faces security vulnerabilities, but also because it requires processing and storing customer voice records in different circumstances. This makes its installation complex and costly for banks with a large number of clients.

It is feasible that future improvements, in combination with other technologies that cheapen the processing and storage of the required information, could allow a more widespread use.

FTP-65. Financial user automated interaction

This product combines artificial intelligence, semantic analysis and cognitive analysis to drive client-financial institution interaction through computer systems, without the need for officials from the financial institution.

Usually the communication between the system and the client is by text, but in others the interaction simulates a voice conversation.

The communication channel, especially in the text version, can be varied: at the financial institution's website, on a mobile phone app, by SMS-USSD messaging, or in social network messaging systems.

Frequently the product is installed in the systems of the financial institution and controlled by it. The fintech firm is limited to giving periodic maintenance to the product.

FTP-66. Digital identification

This is a service that allows individuals' identity verification by accessing a national identification database, if allowed, or private databases. In some cases, it extends the ability to verify documents in public records archives and other documentary databases, allowing companies to be identified.

Usually this service relies on cloud processing, and it depends heavily on online access to databases, in order to offer quick and low-cost results.

FTP-67. Use of data from social networks and other sources to identify people and companies

This is one of the multiple services offered by firms that acquire the information generated by users of social networks, for their processing and analysis. In this case, a non-financial company offers financial institutions to verify that a person or company has activity in social networks, including frequency and location.

Another service is when a client outsources its users' authentication process to a social network, as a way to make use of their own services.

This service is useful for those who offer other fintech products remotely and want to accelerate the incorporation of customers, taking advantage of the reach of social networks, and the abundance of information provided by its users. It can also be used by financial institutions as a complement to their verification processes for new clients.

FTP-68. Innovative compliance software

This product offers the user tools to control compliance with obligations contained in financial regulations, especially those related to the prevention of money laundering, as well as the mitigation of other risks.

In this case, we include those solutions that incorporate artificial intelligence, cognitive analysis, big data analytics and semantic analysis to create alerts and guide the work of those responsible for managing risk in financial institutions.

In some cases, the product is provided as software as a service (SaaS). The non-financial company that develops the software also performs the surveillance activity and alerts the financial institution about suspicious transactions or activities, as well as provides periodic reports.

FTP-69. Innovative risk management solutions

Similar to FTP-68, this product is aimed at financial institutions that wish to complement their existing risk management tools with structured information that the service provider has obtained from other participants in the service, without the need to transmit transaction details or the counterpart's identity.

The service provider ensures that the data has been obtained and distributed in compliance with data and privacy protection regulations. It mostly focuses on the prevention of payment fraud, distinguishing it from the services provided by credit bureaus.

FTP-70. Online accounting

This is a representative software as a service, offering users, primarily small and medium-sized companies, to

run their accounting processes and records in this cloud-based platform.

In addition to the usual accounting functions, it allows for direct integration of other systems, mainly online stores, with the service provider system via API. It is also possible to integrate payments gateways, such as those described in FTP-33. In some cases, it allows automatic bank reconciliation via an API connection with the user's banks.

FTP-71. Online Billing

These are companies that offer online billing service, under the software as a service model. Clients are businesses that must issue electronic invoices in accordance with the tax legislation. In many cases this service is integrated into an online accounting service as described in FTP-70.

Depending on the jurisdiction, companies that offer this type of service require a certification from the tax authority, both as a firm and the software.

FTP-74. Cloud storage based on blockchains

This is a service that allows users to take advantage of available storage space in multiple servers (nodes) in the cloud, in a distributed, encrypted and redundant manner. The files containing the information are initially encrypted, before being sent to the storage server, and divided into a variable number of pieces. Between those who wish to store information and those providing storage, a smart contract is established that sets the conditions of service between each pair of users, such as price, period, availability of the server, etc. The contract, the information that allows to identify the location of the pieces and the fulfilment of the storage conditions is registered in blockchains.

Originally the developers were motivated to offer lower-cost, more accessible and more secure alternatives than traditional cloud storage services. Now it is being used by companies that provide information technology services to corporations, including financial institutions.

Segment: Capital raising

The products included in this segment are services that allow for raising funds from many individuals and firms, with different purposes, but without involving credit. These crowdfunding schemes allow for the financing of initiatives, with or without the return of contributions, which would rarely obtain funds under traditional capital market products. The absence of regulation, however, is reflected in a less than desirable transparency and, consequently, in costs for participants that are comparatively high.

FTP-75. Crowdfunding - real estate

This is an alternative financing scheme (also known as crowdfunding) in which people, individuals or companies, finance or acquire participation in real estate projects. In some cases, the scheme is oriented to recently built buildings.

Like other crowdfunding, the main objective is to gather a high number of investors who place amounts comparatively lower than those that each would require for acquiring any of the assets on offer, while obtaining higher returns than those available in traditional financial instruments.

For real estate developers, this business model has the appeal of being able to finance projects at lower interest rates than what they would probably get in the financial system. The developer may also have quantitative or qualitative restrictions to get bank loans.

Investors, as in the P2P and platforms, can mitigate the counterparty risk associated with the projects, distributing their investment in several projects with different developers.

The company that runs the platform should be independent from developers and should perform both a verification of the existence of the project and its associated risks, as well as an analysis of its financial viability.

The platform operates online, with all transactions taking place over the Internet.

FTP-76. Crowdfunding - capital

Another model of crowdfunding scheme, similar to FTP-75. The difference lies in the company that receives the funds, as in this case they are start-up or planned companies, with a need to expand their capital, issuing shares that are acquired by the investors.

In this model, investors become minority shareholders in companies that do not usually have a defined business model, probably with their main product in an early development phase.

For companies, this scheme allows them to receive funding to cover development expenses without granting controlling stakes to outside investors.

Investors, like in FTP-75, can mitigate the risk of the receiving company failing by distributing their funds among several firms. Due to the greater inherent risk in this type of financing, the platforms are oriented to other businesses or high-net-worth individuals.

In this case, the firm that runs the platform provides limited information on the activities that the companies offering shares carry out or plan to develop, especially key products. For its services, it charges fees to both parties.

These platforms have websites displaying investment opportunities, but in general there are face-to-face or remote rounds of presentations by the firms requesting financing.

WORKING GROUP MEMBERS

Carolus Walters
Centrale Bank van Curaçao en Saint Maarten

Christiano Costa Moreira
Banco Central Do Brasil

Aldo Enrique Matsuoka Tanaka
Superintendente de Banca, Seguros y AFP, Perú

Carolina Flores Tapia
Comisión para el Mercado Financiero, Chile

Nadia Herrera Bellot
Autoridad de Supervisión del Sistema Financiero, Bolivia

Rocío H. Robles Peiro
Comisión Nacional Bancaria y de Valores, México

Thays Bermúdez
Superintendencia de Bancos de Panamá

Marco Antonio Cerrato Cruz
Comisión Nacional de Bancos y Seguros, Honduras

Runako Brathwaite
Central Bank of Barbados

Roberto González Ruíz
Superintendencia General de Entidades Financieras, Costa Rica

Jorge Álvarez Ledezma
Superintendencia General de Entidades Financieras, Costa Rica

Maximir Álvarez
Consultant
International Consulting Consortium, Inc.

ASBA
Marcos Fabián
Antonio Pineda
Ricardo Toranzo

BOARD OF DIRECTORS

Chairman
Paulo Sérgio Neves de Souza
Banco Central do Brasil

Vice Chairman
Jorge Alexander Castaño Gutiérrez
Superintendencia Financiera de Colombia

Director for the Andean Region
Ma. del Socorro Heysen Zegarra
Superintendencia de Banca, Seguros y AFP, Perú

Director for the Caribbean Region
Michelle Francis-Pantor
The Central Bank of Trinidad and Tobago

Director for the Central American Region
Ethel Deras Enamorado
Comisión Nacional de Bancos y Seguros, Honduras

Director for the North American Region
José Antonio Quesada Palacios
Comisión Nacional Bancaria y de Valores, México

Director for the Southern Cone Region
Juan Pedro Cantera Sención
Banco Central del Uruguay

Secretary General
Pascual O'Dogherty

ASBA MEMBERS

ASSOCIATE MEMBERS

Andean Region

Superintendencia Financiera de Colombia
Autoridad de Supervisión del Sistema Financiero, Bolivia
Superintendencia de Bancos del Ecuador
Superintendencia de Banca, Seguros y AFP, Perú
Superintendencia de las Instituciones del Sector Bancario, Venezuela

Caribbean Region

Central Bank of Belize
Banco Central de Cuba
Bank of Guyana
Bank of Jamaica
Banque de la République d' Haïti
Cayman Islands, Monetary Authority
Centrale Bank van Aruba
Centrale Bank van Curaçao en Sint Maarten
Eastern Caribbean Central Bank
Financial Services Regulatory Commission, Antigua y Barbuda
Turks & Caicos Islands Financial Services Commission
Central Bank of Barbados
Central Bank of the Bahamas
Central Bank of Trinidad and Tobago
Centrale Bank van Suriname
Financial Services Commission, British Virgin Islands
Oficina del Comisionado de Instituciones Financieras, Puerto Rico

Central American Region

Superintendencia de Bancos, Guatemala
Comisión Nacional de Bancos y Seguros, Honduras
Superintendencia de Bancos y de Otras Instituciones Financieras de Nicaragua
Superintendencia del Sistema Financiero, El Salvador
Superintendencia General de Entidades Financieras, Costa Rica
Superintendencia de Bancos de Panamá
Superintendencia de Bancos de República Dominicana

North American Region

Board of Governors of the Federal Reserve System, USA
Office of the Comptroller of the Currency, USA
Federal Deposit Insurance Corporation, USA
Comisión Nacional Bancaria y de Valores, México

Southern Cone Region

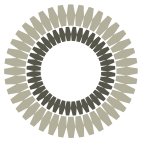
Comisión para el Mercado Financiero, Chile
Banco Central do Brasil
Banco Central de la República Argentina
Banco Central del Paraguay
Banco Central del Uruguay

Non Regional

Banco de España

COLLABORATOR MEMBERS

Banco Central de Reserva de El Salvador
Comisión Nacional de Microfinanzas, Nicaragua
Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, México




ASBA


IDB
LAB