GLOBAL FINTECH REGULATION AND SUPERVISION PRACTICES

Regulation for Responsible and Competitive Financial Sector Innovation

DECEMBER 2019

ASBA
ASSOCIATION OF SUPERVISORS OF BANKS OF THE AMERICAS

IDB | LAB

BOARD OF DIRECTORS

Chairman

Juan Pedro Cantera (until October 2018)
Banco Central del Uruguay

Paulo Sérgio Neves
Banco Central do Brasil

Vice Chairman

José A. Arévalo (until September 2018)
Superintendencia de Bancos de Guatemala

Jorge Castaño
Superintendencia Financiera de Colombia

Director for the Andean Region

Jorge Castaño (until October 2018)
Superintendencia Financiera de Colombia

Socorro Heysen Zegarra
Superintendencia de Banca, Seguros y AFP, Perú

Director for the Caribbean Region

Ingeborg Geduld-Nijman
Central Bank van Suriname

Director for the Central American Region

Ethel Deras
Comisión Nacional de Bancos y Seguros, Honduras

Director for the North American Region

Teresa Rutledge (until October 2018)
Office of the Comptroller of the Currency

José Antonio Quesada Palacios
Comisión Nacional Bancaria y de Valores, México

Director for the Southern Cone Region

Paulo Sérgio Neves (until October 2018)
Banco Central do Brasil

Juan Pedro Cantera
Banco Central del Uruguay

Secretary General

Rudy V. Araujo (until December 2018)

Pascual O'Dogherty

CONTENT

ACKNOWLEDGMENTS

ASBA would like to thank Rudy V. Araujo for his exceptional work and commitment on the *Regulation for Responsible and Competitive Financial Sector Innovation* project in connection with this report.

I. INTRODUCTION

The purpose of this document is to compile and analyze global practices regarding the regulation and supervision of Fintech business models, products and services. To that end, the author reviewed the current regulatory and supervisory practices of financial authorities, building upon a survey distributed among Association of Supervisors of Banks of the Americas (ASBA) members regarding Fintech-related regulations and approaches and other relevant documents.

A total of 56 jurisdictions on all five continents were examined, including 11 within the ASBA membership. The list of jurisdictions is presented in Annex 1.

It should be noted that this report focused on identifying common practices and trends rather than cataloging specific regulations.

The document is structured as follows: Section II studies broad topics regarding Fintech regulation and supervision, such as specific Fintech regulations, authorities' roles in promoting Fintech developments, and prohibitions; Section III explores practices regarding specific Fintech products, while Section IV examines practices regarding technologies that enable many Fintech products; the final section presents some concluding remarks.

II. GENERAL FINTECH REGULATORY AND SUPERVISION PRACTICES

1. REGULATING FINTECH ACTIVITIES WITH THE EXISTING GENERAL FRAMEWORK

In 2018, ASBA distributed among its members a survey[1] regarding the response of regulators to the irruption of Fintech in their financial markets. The answers were analyzed to understand the approaches and future actions in terms of financial regulation and supervision.

At that time, few authorities had issued specific regulations for Fintech products or specialized firms. Although the survey was not exhaustive, fewer than 20 of 38 jurisdictions that submitted a response to the survey, had regulations that could be identified as specific to Fintech.

In part, this paucity of regulatory responses was explained by the relatively small size and lack of material impact of Fintech, as seen by regulators and international bodies such as the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS) and the International Monetary Fund (IMF).

The survey also highlighted that most regulators had adopted a cautious but watchful approach to fully understand the different kinds of Fintech products before attempting to regulate them; keep track of Fintech products and firms' evolution; and strengthen, in staff training plans, the understanding of technological issues related to Fintech and the recruitment of specialized personnel.

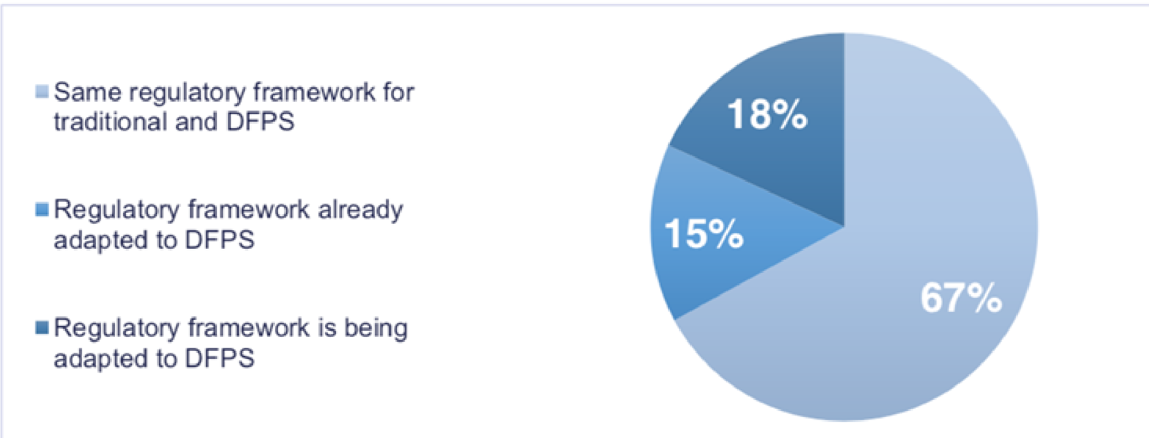
Another explanation is the perception by a majority of authorities that new Fintech products and service providers can or should be accommodated within the current regulatory framework. A survey carried out by the International Financial Consumer Protection Organisation (FinCoNet) among 24 financial supervisors in 23 jurisdictions, including four ASBA members, supports this interpretation.

FinCoNet's report showed that, within the regulatory frameworks for digital financial products and services (DFPS), "only 15% of respondents said they have already adapted their regulatory framework to DFPS. However, this specific adaptation appears to be related only to certain products. Consequently, for the rest of DFPS, these authorities seem to be in a similar situation to the majority of respondents (67%) for which the applicable regulatory framework is generally the same for digital and traditional financial products and services."[2]

1/ ASBA. Identifying Gaps and Opportunities in Financial Innovation Regulation. April 2018.
2/ FinCoNet. Practices and Tools required to support Risk-based Supervision in the Digital Age. November 2018.

The following chart shows the distribution of replies:

GRAPH 1: REGULATORY FRAMEWORK APLPLIED TO DFPS



Source: FinCoNet. Practices and Tools required to support Risk-based Supervision in the Digital Age. November 2018.

Similar results are found in a study among legal firms comparing the international Fintech legal frameworks.[3] None of the 44 jurisdictions surveyed had, at the time of the compilation, a specific Fintech law or general regulation.

This general practice does not preclude the development of regulations for specific Fintech products or firms, chiefly for financial intermediation-like products (P2P and crowdfunding) and electronic payments. A special case is Mexico, where, in March 2018, the legislature passed a broad Fintech law[4] establishing two new types of financial institutions – for crowdfunding and electronic payments – as well as creating the figure of "innovative business models" and authorizing financial authorities to regulate cryptoassets and to grant temporary licenses akin to a regulatory sandbox.

It should be noted that, for regulators following a principles-based approach, extending the existing regulatory and supervisory framework to Fintech is consistent with the 'same-services/activities, same risks, same rules' or 'technology-neutrality' principle. A good example of this view is Switzerland's Financial Markets Supervisory Authority, which has this concept as its starting principle.[5]

The same principle was stated by the European Commission when setting the area's policy on Fintech regulation, which was expressed as "the same activity is subject to the same regulation irrespective of the way the service is delivered"[6]. However, the Commission omitted this principle in a proposal for a European-wide crowdfunding regulation, indicating that an option for "a product-based approach: bringing crowdfunding within the existing EU single rulebook (…) was also not retained, as it would create undue regulatory uncertainty due to the self-regulatory enforcement mechanism".[7]

3/ SUMROY, R. and KINGSLEY, B. (Editors). International Comparative Legal Guide to Fintech v2. Global Legal Group, London, May 2018.

4/ México. Ley para Regular las Instituciones de Tecnología Financiera. March, 9, 2018.

5/ OECD. Reviews of Regulatory Reform: Switzerland. 2006.

6/ European Commission. Consultation Document: Fintech: A More Competitive and Innovative European Financial Sector. 2017.

7/ European Commission. Proposal for a Regulation of the European Parliament and of the Council on European Crowdfunding Service Providers (ECSP) for Business. March 2018.

It should not surprise the reader that this approach is favored by traditional financial institutions, as expressed in their comments to a BCBS' consultation paper Sound Practices: Implications of Fintech developments for banks and bank supervisors.[8]

One advantage of treating Fintech using the existing regulatory and supervisory framework is avoiding the creation of regulatory gaps, which could harm financial services users and traditional and regulated financial institutions.

Another driver of regulators' caution is the uncertainty regarding the extension of the regulatory perimeter to encompass new providers and products or services not explicitly defined within the relevant legal framework.

This uncertainty was also considered by FinCoNet in its survey. A substantial majority of the respondents indicated that there were DFPS and DFPS providers outside the regulatory and supervisory perimeter, as shown in the following graph.

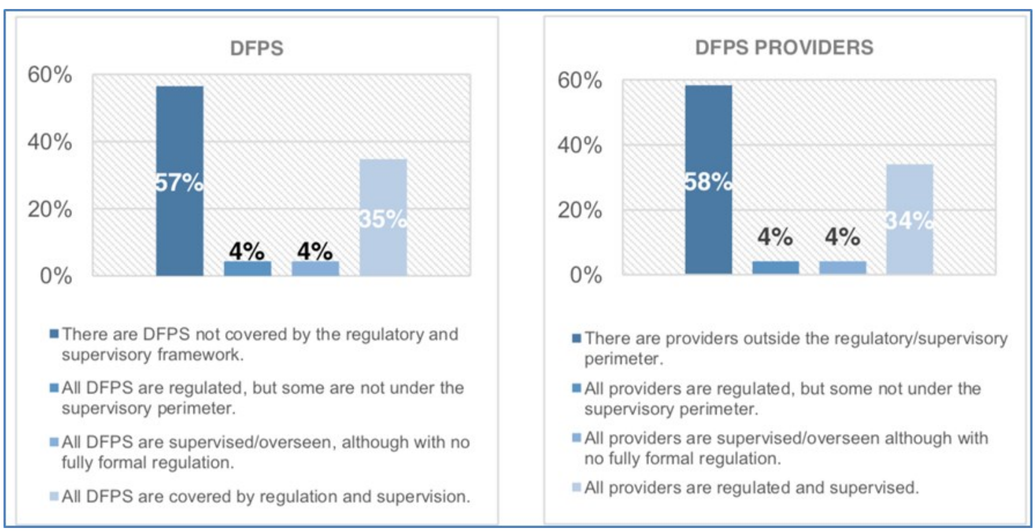
Of course, as has already been noted, regulators have sought to adjust the regulatory perimeter to include new actors and to issue regulations covering specific products, services, and business models, enabling technologies to close regulatory gaps.

The following subsections will examine these regulatory actions.

Whichever the driver, for most regulators, the practice has been to use the existing general regulatory framework when facing the introduction of new products or the appearance of new providers rather than creating a new general regulatory framework.

8/ See comments letters by the International Banking Federation and the World Council of Credit Unions.

GRAPH 2: DFPS / DFPS PROVIDERS AND REGULATORY/SUPERVISORY PERIMETER



Source: FinCoNet. Practices and Tools required to support Risk-based Supervision in the Digital Age. November 2018.

2. BANNING FINTECH PRODUCTS

A direct consequence of the practice discussed above is that supervisors likely examine Fintech products using the existing general financial regulations. Many Fintech products do not exactly fit traditional regulated financial services or products, nor is every Fintech provider a regulated firm. Therefore, this regulatory uncertainty can prompt supervisors to assume that a product and/or its provider is breaking the law.

The risk for Fintech firms of an adverse supervisory action is clear, particularly for those that already have a profitable business model in sight. "Regulatory uncertainty discourages investment. Investors are hesitant to invest in a company that is working in an unregulated landscape as regulatory bodies can swoop in at any time and deem its operations illegal".[9] Therefore, such firms are more likely to advocate for being regulated. A recent survey among Fintech start-ups in Latin America revealed that "thirty-five percent of those surveyed consider regulation necessary, despite the fact that it is presently lacking, compared to only 9 percent who consider that the sector currently needs no specific regulation".[10]

Indeed, there have been supervisory enforcement actions regarding Fintech products and firms. In its mildest form, authorities may discourage consumers from using Fintech firms by stressing that they should only trust licensed firms. In the United States, given its fragmented regulatory and supervisory landscape, this policy can lead to enforcement actions by one state-level authority against Fintech firms licensed in other states, as is the case of the Department of Financial Services of New York State's decision to place restrictions on online lenders unlicensed in that state.[11]

Notwithstanding the perceived risks, supervisors have seldom banned Fintech products or sets of firms. These actions have centered on three types of Fintech products/firms:

- Cryptoassets (the asset class and the firms related to their creation and intermediation)
- Direct distribution of sophisticated financial products to retail users (binary options and contracts for differences)
- Screen, web or data scrapping (a technique to collect financial users' transactional data)

By far, actions restricting or banning cryptoasset transactions have been the most common. Although supervisory practices regarding cryptoassets will be explored in detail later in this report, it is relevant to note here the lack of consensus among authorities on whether to forbid consumers or financial institutions from holding or carrying transactions with cryptoassets. Even among ASBA members, there are clear policy disparities on this issue. On one extreme, Ecuador[12] and Bolivia[13] have banned any transaction with cryptoassets, which is a decision that, in practice, can only be enforced on regulated financial institutions. On the other hand, Mexico's central bank has published a cryptoasset regulation[14] restricting cryptoasset transactions only between regulated financial institutions.

A related topic, although in the securities market, has been prohibitions and restrictions on the so-called Initial Coin Offerings (ICOs), the process of launching and selling new cryptoassets to the general public. Some supervisors, most notably in China and South Korea, reacted by defining these transactions as illegal public securities offerings and issuing blanket bans.

9/ Finextra. The Role of Regulatory Sandboxes in Fintech Innovation. September 2018.

10/ Inter-American Development Bank – Finovista. FINTECH - Latin America 2018 - Growth and Consolidation. 2018.

11/ New York State Department of Financial Services. Online Lending Report. July 2018.

12/ Junta de Politica y Regulacion Monetaria y Financiera. Las operaciones en criptomonedas no están autorizadas en el Ecuador. February 2018.

13/ Banco Central de Bolivia. Comunicado 04/2017. April 2017.

14/ Banco de México. Circular 4/2019. March 2019.

Jurisdictions that have banned cryptoassets, consequently, also ban ICOs. Mirroring the treatment of cryptoassets, some jurisdictions allow ICOs, although they are generally subject to current securities regulations. Examples of this practice are found in Canada, Russia, Singapore, Switzerland and some European Union (EU) countries. The United States does not have a unified approach. The Securities and Exchange Commission treats an ICO as a security offering, but as usually there is no established business supporting the new cryptoasset, it has refused to approve applications. Recently, the Securities and Exchange Commission published a policy statement[15] along with its first 'no-action letter' in effect authorizing an aircraft company to issue a digital token.[16]

On the issue of binary options and contracts for differences, the European Securities and Markets Authority (ESMA) banned[17] the offering of these gambling-linked financial products to retail consumers since the risks involved are poorly understood by unsophisticated investors. Other countries such as Israel[18] and Canada[19] also opted to outright ban such instruments, while New Zealand[20] and Australia allow trading, although the Australian regulator has expressed concern about brokers' practices.[21]

Less extensive is the ban on 'screen scrapping'. This technique requires financial users to provide third parties, usually Fintech firms, with their login credentials at their regulated financial institutions. The Fintech firms then use these credentials to login into the users' bank accounts to capture the transactional data to feed their databases to provide services to their clients. This process creates obvious security risks for users, banks and Fintech firms. The European Union banned this technique as part of the legislation mandating that banks offer third parties more secure and reliable access to their clients' data using an application programming interface (API).[22] This directive, dubbed 'Open Banking', was replicated in the Mexican Fintech law cited above. Other countries have considered a similar move but so far have opted not to ban the technique. The US financial consumer protection authority published a set of principles, including the phrase "access does not require consumers to share their account credentials with third parties",[23] which has been interpreted as signaling a future ban.

Australia, on the other hand, has adopted a more nuanced stance. While recognizing that screen scraping techniques "rely on the consumer (the holder of the bank account) first inputting their internet banking login and password (…) could be viewed as the consumer breaching the standard banking terms and conditions for non-disclosure of passwords to third parties and passcode security requirements in the ePayments Code (…), provided any data security concerns can be addressed, consumers should not be disadvantaged by their use of legitimate account aggregation services".[24]

This cautious view is justified by the resistance by traditional financial institutions to share customers' data even under a legal mandate.

In addition to these general actions, there have been multiple enforcement actions against individual firms using Fintech products to commit fraud or harm consumers. These actions must be seen within the consumer protection framework, which is led by nonfinancial authorities in some cases, and do not reflect practices regarding Fintech per se.

Although supervisors in some cases have banned specific Fintech products, in general, they have abstained from broad bans of Fintech products or firms.

15/ SEC. Statement on Framework for 'Investment Contract' Analysis of Digital Assets. April 2019.

16/ SEC. Response of the Division of Corporation Finance. April 2019.

17/ ESMA. ESMA agrees to prohibit binary options and restrict CFDs. March 2018.

18/ Israel Securities Authority. The Knesset plenum approved second and third reading of the Binary Options Law. October 2017.

19/ Canadian Securities Administrators. Multilateral Instrument 91-102 Prohibition of Binary Options. September 2017.

20/ New Zealand Financial Markets Authority. Binary options. September 2018.

21/ Australian Securities & Investments Commission. ASIC calls on retail OTC derivatives sector to improve practices. June 2018.

22/ European Union. Payment services (PSD 2) – Directive. 2015.

23/ Consumer Financial Protection Bureau. Consumer Protection Principles. October 2017.

24/ Australian Securities & Investments Commission. Review into Open Banking in Australia. September 2017.

3. FINANCIAL AUTHORITIES AS PROMOTERS OF FINTECH

Regulators' open attitude towards Fintech, which was detailed above, reflects a consensus among authorities that Fintech could be useful to promote a fairer, more inclusive and more competitive financial system. In part, this view has been promoted by international bodies. An example is the 'Bali Fintech Agenda', published by the IMF and the World Bank, which states that national authorities should "adapt regulatory framework and supervisory practices for orderly development and stability of the financial system and facilitate the safe entry of new products, activities, and intermediaries; sustain trust and confidence; and respond to risks".[25]

Financial authorities have been implementing a variety of actions to assist those interested in implementing technological innovations in their markets, including developments by incumbent financial institutions, nonfinancial firms and start-ups. Most of these actions can be classified into four sets:

- Setting up a dedicated Fintech unit or at least a direct channel for Fintech-related enquiries;
- Innovation hubs, conceived as a meeting place for authorities, financial institutions and entrepreneurs;
- Setting up a dedicated Fintech unit or at least a direct channel for Fintech-related enquiries;
- Innovation hubs, conceived as a meeting place for authorities, financial institutions and entrepreneurs;

Other activities observed in the review include Fintech policy papers, Fintech incubators in which the financial authority directly assists an aspiring Fintech firm to mature its products, a special Fintech envoy to the parliament and direct assistance to authorities in other countries regarding Fintech issues.[26]

Of the 56 jurisdictions reviewed for this document, over half (32) had at least one program implemented or proposed, including 7 ASBA members.

This finding is not surprising as these jurisdictions were selected for having an active Fintech scene.

It should be noted that, in two countries (Australia and Spain), the schemes were not observed by the entity in charge of supervising banks but by the capital market regulator.
Additionally, in the United States, only two of the federal financial regulators had a special Fintech promotion scheme.

A related topic, although in the securities market, has been prohibitions and restrictions on the so-called ICOs, the process of launching and selling new cryptoassets to the general public. Some supervisors, most notably in China and South Korea, reacted by defining these transactions as illegal public securities offerings and issuing blanket bans.

25/ IMF and World Bank. The Bali Fintech Agenda. October 2018.
26/ NLTimes. New Dutch Fintech envoy named: Former Finance Secretary Vermeend. February 2016. The Government of the United Kingdom also named a special Fintech envoy: HM Treasury. Fixing the foundations: Creating a more prosperous nation. July 2015.

The following table shows the distribution by region and type of scheme:

TABLE 1: OBSERVED FINTECH PROMOTION SCHEMES BY FINANCIAL AUTHORITIES

Continent	Scheme observed	Dedicated unit/ channel	Innovation hub	Regulatory sandbox[27]	Special Fintech license
Europe	14	13	12	9	2
Asia	8	8	6	8	4
Oceania	2	1	1	1	0
Africa	1	1	0	0	0
America	6	4	3	4	3
Total	**32**	**27**	**22**	**22**	**9**
As % of 56 jurisdictions analyzed	57%	48%	39%	39%	16%

Source: Information gathered by the author. Breakdown by jurisdiction in Annex 2.

It is clear that European authorities, or more precisely those belonging to the European Union, are the most proactive promoters of Fintech, followed by Asian jurisdictions. In part, this finding reflects competitive pressures to attract Fintech activity, which in some countries has become national policy.

That is the case of the European Union, where its executive branch, as part of an EU-wide policy, has asked its members "to take initiatives to facilitate innovation (…), [including the] establishment and operation of innovation hubs and regulatory sandboxes".[28] Considering that 12 of the 14 European jurisdictions are members of the European Union, which is in effect a single jurisdiction for this issue, the proportion of jurisdictions with active promotional schemes would be reduced to 47%, mainly in Asia, reflecting the asymmetry of policies between the EU and East Asia, on one hand, and the rest of the world.

Of the four schemes observed, setting up a dedicated Fintech channel is the simplest and cheapest. In some cases, the channel is just a specific email address. Dedicated units can be as small as just three part-time officials.

Innovation hubs, even when started by the financial authority, are usually financed by contributions from other public sector organizations and the industry. On the other side of the spectrum are special Fintech licenses and regulatory sandboxes, which in many jurisdictions, in particular those under a civil law legal regime, require legislative action. Both options are analyzed later in this section.

Therefore, whether a financial authority decides to actively promote Fintech activities depends on the existence of a national policy, the competitive pressure to attract those activities and its technical and financial capabilities.

> The most common and affordable practice, both in legal and financial terms, deployed by authorities willing to promote Fintech activities in their jurisdiction is the creation of a specific communication channel that is staffed by a small but dedicated and well-informed group of officers and is open to those interested in exploring ways to introduce technological innovations into the financial market.

27/ This column includes three countries in which regulatory sandboxes have been proposed but not yet implemented.

28/ European Commission. Fintech action plan. March 2018.

4. REGULATORY SANDBOXES

Perhaps the most emblematic departure from traditional financial supervisory practices has been the regulatory sandboxes implemented by several authorities worldwide. The FSB defines these schemes as "frameworks for testing new technologies in a controlled environment".[29] These regulatory sandboxes have become increasingly popular and are being actively promoted by some countries, Singapore and the United Kingdom in particular, and the industry. To a certain extent, there is the perception that, to attract Fintech activity, a country needs to provide such a scheme.

However, according to FinCoNet, "there are currently no clear and consistent internationally agreed definitions or guiding principles for what constitutes an innovation hub or regulatory sandbox".[30] Additionally, considering that the first sandbox was only established in 2016, the experience gained from these schemes is limited and intrinsically linked to the legal framework of the jurisdictions that have set up sandboxes.

Within the European Union and fulfilling a specific mandate from the European Commission to develop general practices on 'innovation facilitators', the three European Supervisory Authorities (ESAs)[31] prepared a joint report on regulatory sandboxes, concluding that "limited experience has been acquired in the operation of the innovation facilitators referred to in this report as most were established relatively recently. However, some observations can be made further to the results of the comparative analysis and the engagement between the ESAs, the competent authorities and the industry, informing a set of operating principles".[32]

It should be noted that one of the key goals of the report is to ensure convergence among the EU national authorities in these schemes. The European Commission, when it instructed the ESAs to study regulatory sandboxes, recognized that "national authorities expressed mixed views: some supervisors consider that such initiatives are not part of their mandate; supervisors that are open to sandboxes, by contrast, consider that others should take similar initiatives".[33]

In other jurisdictions, the use of regulatory sandboxes by supervisors is also being disputed, most notably in the United States. The fragmented financial regulatory landscape in that country has been identified by the federal government and the industry as a barrier to innovation. This finding has prompted the US Treasury to recommend "that federal and state financial regulators establish a unified solution that coordinates and expedites regulatory relief under applicable laws and regulations to permit meaningful experimentation for innovative products, services, and processes. Such efforts would form, in essence, a 'regulatory sandbox'".[34]

The financial supervisor directly under the direction of the US Treasury, the Office of the Comptroller of the Currency (OCC), promptly responded by proposing a new type of banking license: a 'special purpose national bank'. According to the OCC, this "is a national bank that engages in a limited range of banking or fiduciary activities, targets a limited customer base, incorporates nontraditional elements, or has a narrowly targeted business plan".[35]

The New York State Department of Financial Services reacted to this idea by expressing that the state-level supervisor "fiercely opposes the Department of Treasury's endorsement of regulatory 'sandboxes' for financial technology companies.

29/ Financial Stability Board. Financial Stability Implications from Fintech. June 2017.

30/ FinCoNet (2018).

31/ The European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA), collectively known as the ESAs.

32/ ESASs. Joint report on regulatory sandboxes and innovation hubs. January 2019.

33/ European Commission (2018).

34/ US Treasury. Nonbank Financials, Fintech, and Innovation. July 2018.

35/ OCC. Considering Charter Applications From Financial Technology Companies. July 2018.

The idea that innovation will flourish only by allowing companies to evade laws that protect consumers, and which also safeguard markets and mitigate risk for the financial services industry, is preposterous. Toddlers play in sandboxes. Adults play by the rules. Companies that truly want to create change and thrive over the long-term appreciate the importance of developing their ideas and protecting their customers within a strong state regulatory framework".[36]

The Consumer Financial Protection Bureau (CFPB) also announced its intention to set up a regulatory sandbox,[37] following Treasury's recommendations. Among the several comments received in the consultation, a letter signed by 22 state attorneys general stands out by concluding that "innovation should not come at the expense of consumers or the stability of the U.S. financial system. If the financial crisis taught us anything, it is that regulators should be wary of innovations in the financial sector until they can comprehensively evaluate their risks. Moreover, events in the recent past do not inspire confidence that companies in the financial and technology industries are capable of policing themselves. Unfortunately, the Proposed Policies embody precisely the type of blind faith in industry and regulatory diffidence that the CFPB was created to correct, and we urge you to rescind them".[38]

In view of the short history of regulatory sandboxes; their legal, technical and staffing requirements and the opposing views these schemes create, it is not possible to present the observed characteristics as general practices. Nevertheless, acknowledging the interest this scheme has created among supervisors and bearing in mind that three members of the ASBA – Barbados,[39] Colombia[40] and Mexico[41] – have implemented regulatory sandboxes and that others are considering this option, the lessons and practical advice provided by those operating sandboxes will be reviewed in future reports.

5. SPECIAL FINTECH LICENSING

As mentioned, some jurisdictions have introduced a new class of Fintech-related licenses. These licenses can fall within two large groups. On one hand, a few jurisdictions, such as Mexico,[42] Dubai[43] and the US,[44] have implemented their regulatory sandboxes by requiring unlicensed firms to apply for a specifically tailored license. This approach contrasts with that adopted by most authorities operating sandboxes, which either exempt aspiring firms from obtaining a license before testing (i.e., Australia and Singapore) or require the firms to apply for a regular license (United Kingdom). These sandbox-linked licenses are time limited, are usually product specific and have explicit exit conditions.

On the other hand, some authorities offer Fintech firms a permanent special license with less stringent regulatory requirements than those of standard financial licenses. The goal of these licenses is to allow new entrants to effectively compete with incumbent financial institutions while satisfying key elements of the standard licensing framework. In some jurisdictions,[45] this type of license coexists with those linked to regulatory sandboxes; the first aimed at providers with more mature Fintech products than those wanting to test their products in a sandbox.

36/ VULLO, M. T. Statement by DFS Superintendent. July 2018.

37/ CFPB. Policy on No-Action Letters and the BCFP Product Sandbox. December 2018.

38/ New York State Attorney General's Office. Comment Submitted. February 2019.

39/ Central Bank of Barbados. Regulatory Sandbox. Started in October 2018.

40/ Superintendencia Financiera. La arenera. Started in April 2018.

41/ México. Ley para Regular las Instituciones de Tecnología Financiera. March 9, 2018.

42/ Idem.

43/ Dubai Financial Services Authority. The DFSA Rulebook General Module – Amendment. May 2017.

44/ OCC (2018).

45/ Most notably Mexico.

Some jurisdictions, if their legal framework allows, simply waive some requirements of standard licenses to reduce the regulatory burden on new financial institutions. For example, South Korea's Financial Services Commission indicated that it "will grant new online-only banks a grace period of two or three years for the implementation of Basel III regulations, (…) the deferral is to give new online-only banks time to adapt to a new regulatory regime, easing their regulatory burden at the early stage of business operation".[46]

Other authorities set operational restrictions and regulatory waivers for those obtaining a Fintech license, as illustrated by the Swiss Fintech license, which limits the size of individual deposits[47] and forbids interest payments.

However, the widely adopted approach to Fintech firm licensing is to issue product-specific authorizations, usually within two broad camps: payment services and innovative lending. Although not initially conceived specifically for Fintech firms, payment-related licenses are both almost universally available and suitable for many Fintech products.

Moreover, for many Fintech start-ups and nonfinancial big technological companies, obtaining a payment services provider license could be seen as a first step to entering the regulated financial market. Monzo Bank and Starling Bank in the United Kingdom and PayU in India are examples of start-ups with an initial license limited to payment services that later started offering loans and accepting deposits, becoming full-services online banks. So far, all Big Tech forays into financial services have begun with payment services licenses, such as Alibaba and Tencent in China, while Amazon, Facebook, Google and Microsoft have all obtained 'money transmitter' licenses in the US. Additionally, these firms, except Tencent, have obtained a payment services provider license in the European Union. "Thereafter, some expand into the provision of credit, insurance, and savings and investment products, either directly or in cooperation with financial institution partners".[48]

For supervisors, on the other hand, payment services regulation and supervision have a long and trusted track record, and the risks are better understood.

Therefore, offering a license restricted to payment services could be seen as a safe route to ensuring that firms lacking financial expertise progressively acquire the necessary skills before they are allowed to accept deposits and lend money.

Among the 56 jurisdictions analyzed for this document, 44 have a payments-only license; in many cases this license is adapted to cater to Fintech firms. Less common are P2P or crowdfunding licenses, which are used in approximately one-third of jurisdictions. Just three jurisdictions have launched either a cryptoasset-related or virtual bank license. It should be noted that the payments category includes e-money issuing, local and international electronic transfers and mobile wallets.

Additionally, the European Union has issued directives regarding e-money[49] and payment services[50] and is considering an EU-wide directive on crowdfunding and P2P,[51] which would establish special licenses for these areas. Thus, all EU member states as well as those belonging to the European Economic Area[52] (EEA) have or will have incorporated these directives into their national legislation.

The analysis considered whether the licensing regime was distinctive enough to deem it adapted for Fintech products and firms and disregarded those cases in which the regulation and/or the authority approach were indistinguishable from traditional licensing schemes.

46/ Financial Services Commission. FSC to delay implementation of Basel III for new online-only banks. March 2019.

47/ Swiss Financial Market Supervisory Authority. Fintech licence. March 2018.

48/ FROST, J. et al. BigTech and the changing structure of financial intermediation. BIS Working Papers No 779. April 2019.

49/ European Union. E-money - Directive 2009/110/EC. September 2009.

50/ European Union. Payment services (PSD 2) - Directive (EU) 2015/2366. November 2015.

51/ European Commission. Legislative proposal for an EU framework on crowd and peer to peer finance. March 2018.

52/ The EEA includes all EU countries and Iceland, Liechtenstein and Norway. It allows these countries to be part of the EU's single market while adopting all EU regulations. For more information, see European Economic Area (EEA) / Relations with the EU.

The following table shows the prevalence and geographic distribution of Fintech special licenses:

TABLE 2: OBSERVED FINTECH LICENSING SCHEMES

Continent	Payment	P2P	Crowdfunding	Cryptoassets	Virtual bank	Jurisdictions analyzed
Europe	20	5	8	1	0	23
Asia	11	5	3	1	3	13
Oceania	0	1	1	0	0	2
Africa	5	0	0	0	0	7
America	8	3	5	1	0	11
Total	**44**	**14**	**17**	**3**	**3**	**56**
As % of 56 jurisdictions analyzed	79%	25%	30%	5%	5%	100%

Source: Information gathered by the author. Breakdown by jurisdiction in Annex 3.

From these results, it is clear that it is a common practice to have a Fintech-compatible payments services license. The same cannot be said of P2P or crowdfunding-oriented licenses. Even rarer are licenses for cryptoasset-linked intermediaries or issuers or for online-only banks.

6. PRACTICES REGARDING FINTECH CROSS-BORDER PROVISION

Almost every jurisdiction examined legally forbids the cross-border provision of financial services if the provider is not authorized by a local supervisor.

There are some exceptions to this general practice that are worth mentioning. The European Union, including the EEA, allow for full access in any of its members to financial institutions licensed in another, which is a feature known as ‘passporting rights’ and is consistent with the concept of a single EU-wide financial market. In addition, the Markets in Financial Instruments and Amending Regulation[53] allows for the provision of specific financial services by non-EEA firms without a branch or license. The range of services is narrow and is mostly linked to wholesale capital markets, such as OTC derivative trading, hedging and similar transactions.

Although the regulation does not exclude or mention Fintech products, there are no known Fintech firms using this capability.

The other notable exemption to the general practice is Switzerland. “Swiss banking and anti-money laundering regulations do not apply to Fintech operators that are domiciled abroad and offer their services into Switzerland on a pure cross-border basis, that is without employing persons permanently on the ground in Switzerland and without establishing a branch or representative office or any other form of relevant physical presence in Switzerland”.[54]

53/ European Union. Directive 2014/65/EU. May 2014, in force since early 2018.

54/ HSU, P. and FLÜHMANN, D. Regulating innovation. International Financial Law Review. April 2017.

Likewise, Bank Negara Malaysia's regulatory sandbox "is open to all Fintech companies including those without any presence in"[55] that country.

Nevertheless, previous reports have highlighted how the technologies underpinning many Fintech products allow for the provision of financial services and products to users in a country by a firm without a physical or legal presence in that country. Many authorities recognizing that blocking access to financial services or products provided electronically from abroad can be difficult in the absence of capital controls, have sought to establish a cooperation mechanism with the supervisor of the countries of origin of Fintech product providers.

The use of Fintech-specific memorandums of understanding (MoUs) between supervisors is a common approach globally. A further step has been to include not only supervisors but also other authorities and market participants in bilateral cooperation agreements or 'Fintech bridges'.[56] According to one analyst, 63 bridge agreements have been signed, covering most regions, as this map shows:

55/ Bank Negara Malaysia - Financial Technology Enabler Group. FAQ.
56/ See: UK-Australia Fintech Bridge.

GRAPH 3: FINTECH BRIDGES

Source: KAE. Fintech Bridges across the Globe.

The intangible nature of Fintech products, telecommunications networks' global reach and the absence of capital control in most countries underline the high probability that users are being provided with Fintech products from outside their jurisdiction. Therefore, it is clear that financial authorities seek Fintech-specific MoUs to expedite cooperation from home supervisors of such providers. At the same time, recognizing that Fintech transcends the sphere of financial markets, these authorities are seeking to involve other authorities in these agreements to ensure a unified and informed response to the cross-border provision of financial services.

7. PRACTICES REGARDING AML/CFT ISSUES

Of all the topics discussed in this chapter, the regulatory and supervisory approach to antimoney laundering/ countering financial terrorism (AML/CFT) in the context of Fintech products and firms is the most homogeneous among the jurisdictions examined. To a large extent, this uniformity reflects the ongoing efforts by international bodies, in particular the Financial Action Task Force (FATF),[57] to analyze the challenges posed by Fintech to the traditional AML/CFT practices and, then, adjusting their recommendation to address the perceived gaps.

In the analysis of this issue, we found that in several jurisdictions, even Fintech activities outside the regulatory perimeter of financial supervisors have been subject to AML/CFT obligations by other authorities, which were helped by the broad range of activities covered by national AML/CFT legislation.

This practice aligns with the FATF approach to Fintech, which identifies three areas of concern:

- Cryptoassets
- Distributed Ledger Technology
- Digital Identification

Firms and individuals involved in cryptoassets, who are sometimes reluctant to be regulated, have been increasingly forced to comply with AML/CFT regulations akin to those applied in the financial sector without prejudice to their regulatory status as financial actors.

The general practice regarding AML/CFT cryptoasset firm regulations is to mandate, as a minimum, strict client identification and source of funds verification procedures at cryptoassets trading platforms, where fiat currency and cryptoassets are exchanged, as well as requiring the firms operating the platforms to comply with the standard reporting requirements. Many jurisdictions also require cryptoasset firms to have a compliance officer.

With respect to other Fintech activities, similar practices have been identified. However, the de-risking trend observed in several jurisdictions has in some cases affected the development of Fintech.

In its first report on the results of the first regulatory sandbox in the United Kingdom, the Financial Conduct Authority (FCA) stated the following:

"We have witnessed the denial of banking services first-hand across a number of firms in the first two cohorts of the sandbox. Difficulties have been particularly pronounced for firms wishing to leverage DLT [distributed ledger technology], become payment institutions, or become electronic money institutions. We are concerned by what appear to be blanket refusals for certain kinds of applicant firms. There are also apparent inconsistencies within individual banks regarding how they apply their assessment criteria in approving access to banking services".[58]

57/ FATF. Fintech & RegTech Initiative.

58/ FCA. Regulatory sandbox lessons learned report. October 2017.

In several developing economies, the jurisdictions reviewed were identified as using a combination of risk-based approaches and proportionality in the AML/CFT regulation of key Fintech products and firms linked to financial inclusion. In these cases, Fintech-related technologies are seen by the supervisor as a solution to some claims expressed by incumbent financial institutions about perceived weaknesses in AML/CFT controls in new Fintech firms, especially clients' onboarding practices and remote know your client (KYC) procedures. Sometimes it is difficult to separate genuine concerns, such as the general 'de-risking' trend observed in many developing countries, from barriers to potential competitors.[59]

A common practice deployed by supervisors to avoid excessive AML/CFT-based restrictions on Fintech firms is the introduction of simplified accounts coupled with a simplified KYC process allowing agents to perform initial due diligence regarding new customers and, in some cases, biometric identification technology.[60]

8. CYBERSECURITY

The risk of a financial institution being subject to criminal attacks through communication channels and data processing centers has been growing significantly in recent years. Although this is not a specific Fintech issue, Fintech is undoubtedly increasing the reliance on automated and electronic systems in the provision of financial services. Both new Fintech firms and traditional financial institutions are exposed to cyberattacks as is the point at which these two sets of firms interact. Additionally, "Fintech firms are increasingly attractive targets and typically have fewer resources dedicated to cybersecurity, as they prioritize growth and product-market fit".[61]

This emerging trend has prompted financial authorities to adapt both the regulatory framework and their supervision tools to ensure that all participants in the financial markets maintain a minimum level of security.

This emerging trend has prompted financial authorities to adapt both the regulatory framework and their supervision tools to ensure that all participants in the financial markets maintain a minimum level of security. Managing cybersecurity risk is seen as part of the broader operational risk management process. As such, the evaluation and mitigation activities include not only activities within regulated institutions but also activities at firms providing electronic services to the former.

The initiative of the World Bank to compile regulatory and supervision practices[62] and research on the topic[63] have highlighted how relevant this issue has become. These regulatory and supervisory practices included in these documents are not Fintech specific, although it is clear that Fintech products have motivated some recent developments. It is worth mentioning the following actions:

The Reserve Bank of India, in 2016, issued a 'direction'[64] to nonbanking financial companies that act as 'account aggregators', which is defined as "the service of retrieving or collecting (…) financial information pertaining to its customer".[65] The document specifies the risk management framework that these companies must have as well as mandating that they "shall adopt required IT framework and interfaces to ensure secure data flows from the Financial Information providers to its own systems and onwards to the Financial Information users".[66]

59/ Alliance for Financial Inclusion. Stemming the tide of de-risking through innovative technologies and partnerships. 2016.

60/ Alliance for Financial Inclusion. Proportionality in Practice. Case Studies (Volume 1). August 2018.

61/ Ng, C. Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy. February 2018.

62/ World Bank. Financial Sector's Cybersecurity: A Regulatory Digest. October 2017.

63/ Almansi, A.A. Financial sector's cybersecurity: regulations and supervision. January 2018.

64/ Reserve Bank of India. Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions. 2017.

65/ Idem.

66/ Idem.

Another example of a cybersecurity practice linked to Fintech is the United Kingdom's 'Open Banking' scheme. As in the previous case, this scheme sets the framework for exchanging financial information between financial institutions and third parties. The British authorities have opted for a mix of regulations[67] and standards. The Open Banking Implementation Entity (OBIE), a company created by the Competition and Markets Authority, has defined an 'OBIE Standard'[68] that includes specific security methods and risk management tools. Participants in the program, both financial institutions and other third parties, mostly Fintech firms, must obtain a 'conformance and certification' from the OBIE to become a participant program.

In parallel, the FCA takes into account the implementation of the standards while supervising participants. The supervisor verifies, among other areas, incident management procedures, the adequacy of the mitigation measures and the control mechanisms implemented. The FCA expects that the supervised firm's "approach to operational and security risk management should be proportionate to its size and the nature, scope, complexity and riskiness of its operating model, and of the payment services it offers".[69]

It should be noted that these practices are supported by the national cybersecurity agency,[70] which provides technical assistance and crisis management support to individuals and organizations, including financial institutions.

Another example of an approach to cybersecurity combining regulations and support to raise the capabilities of financial institutions to adequately manage cybersecurity is the Hong Kong Monetary Authority's (HKMA) Cybersecurity Fortification Initiative. This scheme includes "a common risk-based assessment framework for Hong Kong banks, a professional training and certification programme that aims to increase the supply of qualified professionals, and a cyber-intelligence sharing platform".[71] At the same time, the HKMA is explicitly expecting that supervised firms enhance "their cybersecurity cultures by equipping staff with the right skills, the right knowledge and the right behaviour".[72]

Although the HKMA emphasizes that this is not a mandatory requirement, it fits with the general supervisory approach to e-banking risk management.[73]

Similar requirements regarding cybersecurity skills by board members and staff have been implemented by the Monetary Authority of Singapore (MAS). The policy document states that the supervisor "expects that the Board be regularly apprised on salient technology and cyber risk developments",[74] which is a requirement that is well suited to traditional financial institutions engaging with Fintech firms or implementing Fintech products.

Latin America and the Caribbean are not immune to cyberattacks. A report by the Organization of American States (OAS) indicates that at least 9 out of 10 banking entities suffered cyber incidents during 2017; 37% of the banks in the region were victims of successful attacks, and 39% of the incidents were not reported. According to the report, underreporting is particularly prevalent among medium and small banks. The report also indicates that the average cost for a financial institution to recover from a cybersecurity incident is US$1.9 million, although the figure for large banks is much higher, US$5.3 million. In contrast, expenditures on cybersecurity are relatively smaller as a proportion of EBITDA than those observed in other regions. The report highlights that 62% of the banks surveyed indicated that their expenditure on cybersecurity protection increased from the previous year because of regulatory requirements.

67/ UK Treasury. The Payment Services Regulations. 2017.

68/ Open Banking. Open Banking Standard.

69/ FCA. Payment Services and Electronic Money – Our Approach. December 2018.

70/ National Cybersecurity Centre.

71/ HKMA. Guide to Enhanced Competency Framework on Cybersecurity. January 2019.

72/ Idem.

73/ HKMA. Supervisory Policy Manual Risk Management of E-banking. September 2015.

74/ MAS. Circular on Technology risk and cyber-security training for Board. October 2015.

These findings contrast with the significant proportion of clients that regularly use digital channels to conduct financial transactions, 88%. It should be noted that 27% of the users surveyed expressed that the confidentiality, integrity or availability of their information or their financial resources was compromised by their bank, with 43% of these suffering financial losses as a consequence.

The report concludes by recommending that authorities "issue guidelines, recommendations and instructions, as the case may be, derived from the periodic review of best practices and/or applicable international standards regarding digital security, as well as the international regulatory framework applicable to the banking sector, and if necessary issue the necessary legal instruments for application".[75]

It is not surprising that a number of financial authorities in Latin America and the Caribbean, prompted by high-profile cyberattacks, have implemented cybersecurity actions mostly as regulations. That was the case in Mexico, where the financial supervisor, the National Baking and Stock Commission (CNBV) revamped its regulations after a high-profile cyberattack on banks. The changes apply to lending institutions[76] including the two 'financial technology institutions'[77] created by the 'Fintech law' of 2018, although the emphasis is on 'collective financing institutions', which covers both P2P and certain types of crowdfunding.

Among the most notable changes are the obligation to appoint a 'Chief Information Security Officer', a mandatory biannual penetration test performed by an independent specialist firm alongside quarterly in-house tests and the notification to the supervisor of any 'security incident' within 60 minutes of the institution becoming aware of it. Additionally, the reformed regulation expanded the operational risk management framework, introducing a new annual security master plan and specific cybersecurity-related duties for the top executive at the institution. The CNBV separately issued these cybersecurity rules for traditional financial lenders and newer Fintech firms. Although both versions contain similar requirements, the regulations for traditional financial institutions are more specific.

The financial supervisor in Chile also expanded its risk management guidelines to include cybersecurity. The supervisor expects the management and the board to regularly "detect, investigate and generate actions to mitigate the impact of these events, and safeguard the confidentiality, availability and integrity of their information assets".[78] Additionally, the regulation sets specific requirements to notify the supervisor and the affected users, and it imposes a "duty of banks to share information about attacks related to cybersecurity."[79]

Both Latin American regulations, when compared to the cybersecurity practices identified elsewhere, are far more prescriptive, reaching a level of detail absent in the guidelines mentioned in Hong Kong or the United Kingdom.

75/ OAS. State of Cybersecurity in the Banking Sector in Latin America and the Caribbean. 2018.

76/ CNBV. Disposiciones de carácter general aplicables a las instituciones de crédito. Reformed in November 2018.

77/ CNBV. Disposiciones de carácter general aplicables a las instituciones de tecnología financiera. Reformed in March 2019.

78/ Superintendencia de Bancos e Instituciones Financieras Chile. Recopilación actualizada de normas. Capítulo 1-13. 2013.

79/ Superintendencia de Bancos e Instituciones Financieras Chile. Recopilación actualizada de normas. Capítulo 20-8. 2018.

III. PRACTICES REGARDING SPECIFIC FINTECH PRODUCTS

1. E-MONEY

Among Fintech products, those involving electronic money issuance, mobile payments and value storage by nonbanks have been regulated and supervised the longest. Therefore, it is not surprising that there is already a substantial body of best practices closely followed by authorities worldwide. For the purpose of this section, e-money includes the following Fintech products: mobile phone banking, mobile networks operators (MNO) and financial institution convergence, digital wallets on mobile devices, virtual prepaid cards, mobile payments, mobile payments direct cooperation bank - mobile network operator, mobile payments - direct billing to mobile, and text messaging-based mobile payments.

One source of regulatory convergence in this area has been the Digital Financial Services Working Group, compromising financial supervisors from countries with a financial inclusion goal.

This Working Group declares that one of its key objectives is to "stimulate discussion and learning on new approaches, and good practices in DFS [Digital Financial Services] regulation".[80]

The presence of large international MNOs has also contributed to this harmonization, as they are the key providers of these products in many developing economies.

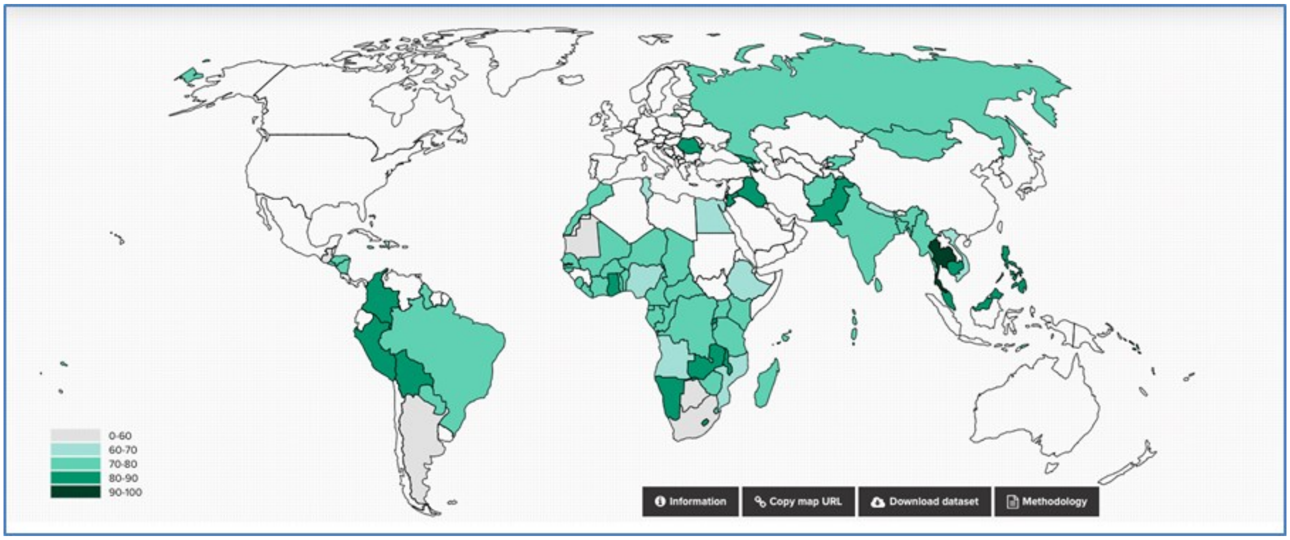
The international MNO trade body, the Global System for Mobile Communications (GSMA), has been promoting an international common approach to the regulation of mobile money. The GSMA produced a "Mobile Money Regulatory Index [that] measures regulatory enablers of mobile money adoption".[81] The following graph shows the index results for 80 jurisdictions that were the focus of the study.[82]

80/ Digital Financial Services Working Group. Fact sheet. July 2018.

81/ GSMA. Mobile Money Regulatory Index – Methodology. September 2018.

82/ Countries in white were not analysed, even though many of them have mobile money regulations, as in the case of Mexico.

GRAPH 4: MOBILE MONEY REGULATORY INDEX



Source: GSMA. Regulatory Index. Consulted on April 2019.

By combining the information directly obtained from the surveyed jurisdictions with the GSMA database on mobile money regulation, a set of practices clearly emerged.

Nonbanks are allowed to provide e-money services directly or through a subsidiary.

Only a few countries allow providers to engage in other financial or nonfinancial activities. However, it is worth noting that, in Kenya, the birthplace of mass mobile money, the provider (Safaricom) is offering other financial products in joint ventures with regulated banks.[83] Additionally, in the European Union, a few Fintech firms that started as e-money providers have transitioned to full commercial banks, such as Wirecard Bank in Germany and Starling Bank in the United Kingdom.

To engage in e-money services, providers require a formal authorization with a different and less stringent set of requirements than those applied to traditional financial institutions.

Following the successful experience of Safaricom's m-Pesa mobile money service in Kenya, almost every jurisdiction surveyed has created a license for e-money providers. It is worth noting that the European Union set an initial capital requirement of 1 million euros in its first e-money directive.[84] In 2009, the EU lowered the requirement to €350 thousand, and in 2015, it introduced a tiered scheme with a minimum initial capital requirement of just €50 thousand for 'small' providers.[85]

Customer funds are segregated from the provider's own funds. In most cases, the funds are held at a regulated financial institution as deposits or in trusts.

83/ CGAP. Top 10 Things to Know About M-Shwari. April 2015.
84/ European Union. Directive 2000/46/EC. September 2000.
85/ European Union (2015).

Some jurisdictions require providers to diversify the customer funds, in several institutions and/or instruments. An example is Kenya that requires "a payment service provider (…) to employ appropriate risk mitigation strategies to ensure that the funds held in the Trust Fund are sufficiently diversified.[86]

The financial services consumer protection framework covers e-money services.

Besides the protection against provider's insolvency covered by the segregation of funds, almost all jurisdictions have extended the consumer protection framework perimeter to include licenced e-money services. This allows for similar procedures and rights regarding financial misconduct. However, some studies have detected that "consumers are not sure who to approach if and when they have complaints related to mobile money, especially when they involve the MNO".[87]

E-money providers are subject to AML/CFT regulations and oversight.

In all the jurisdictions reviewed, the providers of e-money must comply with AML/CFT regulations. Depending on the specific legal framework and supervisory arrangement, compliance can be verified by different authorities. This is the case in the United States, where e-money services providers can be supervised by either Federal or State-level authorities. In some states, 'money services business' (MSBs) are unregulated. This situation is reflected in an evaluation by the FATF, which indicates that "the regulatory and supervisory framework in the U.S. is highly complex and multi-faceted, involving a number of authorities both at the Federal and State levels".[88] Nonetheless, the report recognizes that "the process of coordinating MSB examinations between Financial Crimes Enforcement Network (FinCEN), Internal Revenue Service (IRS) Small Business/Self-Employed (SBSE) and the States is positively evolving. FinCEN and IRS SBSE have taken initiatives to address unregistered money remitters through outreach and enforcement actions, which have been effective".[89]

The regulation allows e-money providers to use agents to perform transactions. The provider must inform and, in most cases, seek authorization from the supervisor before using an agent. The e-money provider must agree to assume any liability for losses to customers caused by the agents.

Some jurisdictions, for example Bangladesh,[90] restrict the range of activities that agents can perform, such as cash-in and cash-out. In other cases, such as Ghana,[91] agents can enroll new customers and perform basic KYC processes, often within a tiered agent scheme.

2. P2P, CROWDFUNDING AND OTHER FINANCIAL INTERMEDIATION PRODUCTS

Fintech products that involve financial intermediation are, after payment-related products, the most fertile ground for regulatory and supervisory activity worldwide, albeit with a lesser degree of consensus among authorities. The set of Fintech products reviewed in this section are as follows: own funds lending to consumers and businesses; P2P to consumers and businesses, and a set of crowdfunding services, including equity, real estate, donations and rewards.

First, it is important to point out that, in most jurisdictions, donation and reward crowdfunding are seldom regulated, as they are not considered financial products as long as the person providing the funds does not expect a monetary return.

86/ Kenia National Treasury. The National Payment System Regulations. 2014.

87/ United Nations Conference on Trade and Development. Mobile Money for Business Development in the East Africa Community. 2012.

88/ FATF. AML/CFT measures - United States - Mutual Evaluation Report. December 2016.

89/ Idem.

90/ Bangladesh Bank. Bangladesh Mobile Financial Services (MFS) Regulations. July 2018.

91/ Bank of Ghana. Agent Guidelines. July 2015.

However, the UK's FCA subjects both types of crowdfunding activities to its payment regulation, including the AML/CFT rules.[92] Similarly, Switzerland requires a crowdfunding platform, regardless of its objective, to obtain a banking license if it "accepts funds on a commercial basis and, rather than forwarding them to the project developer within 60 days (…), holds them for some time [and] the funds accepted for forwarding do not exceed CHF 1 million".[93]

Another important demarcation is regarding balance sheet lending platforms, FTP-01 and FTP-02, which are usually left unregulated or regarded as other traditional non deposit-taking finance companies.

The regulatory treatment of the other products (P2P and equity/real estate crowdfunding) is less clear. A study by the OECD remarked that "different countries have chosen different regulatory approaches towards lending-based crowdfunding platforms. A number of countries have set-up a specific legislation to explicitly regulate lending-based crowdfunding platforms (France, the UK and Israel). Other countries have introduced crowdfunding regulation that either applies to both lending-based and investment-based crowdfunding or appears to not distinguish between the two business models (Austria, Belgium, Finland, Mexico, Portugal). The EU proposal falls into the latter category".[94]

These differentiated approaches probably stem from the priorities and market realities of regulators. As a commentator noted in 2013, "it is interesting to see that while the US regulators have been creating regulation around equity crowdfunding as part of the JOBS Act, the UK regulators have been concurrently designing regulation around p2p lending".[95] In the case of the UK, the emphasis on P2P lending was undoubtedly connected with the traditional banks' withdrawal from Small to Medium Sized Enterprises (SME) lending after the banking crisis, whereas, in the US, the role of capital markets in business financing was a determinant for the initial interest in equity crowdfunding.

Despite the differences between equity crowdfunding and P2P lending, a common practice is to require platform providers to warn customers that returns are not guaranteed and that they could lose their investment if the borrower or the firm receiving the investment fails. Additionally, the providers must clearly state that the funds invested are not protected by a deposit guarantee scheme.

This requirement is enforced even in those cases where the provider sets up a 'provision fund' to cover expected losses.

Additionally, in most regulations for both P2P and equity crowdfunding, "the regulation often specifies that clients' money should be held in a special trust account (e.g., Israel and Mexico), or in most countries platforms do not even have the right to handle clients' money and should rely on a payment institution or obtain a license of a payment institution to do this".[96]

Looking specifically at P2P lending, its regulation and supervision is still a work in progress, with some authorities redeveloping their regulations; most notably, the UK's FCA is currently developing its second generation of regulation to address weaknesses in its first regime from 2014. One area of concern is ensuring that the failure of P2P platforms does not harm costumers. A review of the regulatory framework stated that "so far, losses and defaults across the P2P sector have been low. However, it is important to recognise that the sector is still relatively new and has not been through a full economic cycle. When economic conditions tighten, losses on loans and investments may increase. The sector has not yet been through such a tightening and so the resilience of the P2P business models observed remain relatively untested".[97]

92/ FCA. Crowdfunding and authorisation. August 2017.

93/ FINMA. Crowdfunding. August 2017.

94/ HAVRYLCHYK, O. Regulatory Framework for the Loan-Based Crowdfunding Platforms. November 2018.

95/ RENTON, P. New UK Regulation Provides a Best Practices Template for P2P Lenders. October 2013.

96/ HAVRYLCHYK (2018).

97/ FCA. Loan-based ('peer-to-peer') and investment-based crowdfunding platforms: Feedback on our post-implementation review and proposed changes to the regulatory framework. July 2018.

This concern led the FCA to propose strengthening the current mandate to ensure that existing loans can continue to be managed in the event of platform failure. Specifically, the FCA proposes a ‘P2P resolution manual’ with content similar to that of the so-called living wills required for systemic important financial institutions:

- “critical staff and their respective roles
- critical premises
- IT systems
- record keeping systems, including how records are organized
- all relevant bank accounts and payment facilities
- all relevant persons outside the platform and their respective roles, including any outsourced service providers and
- all relevant legal documentation, including customer, service and supplier contracts
- a group structure chart
- the steps that would need to be implemented under the wind-down arrangements
- any terms in contracts that may need to be relied upon and
- how the platform’s systems can produce the detail specified in respect of ongoing disclosures”.[98]

Similarly, in France, platforms are required to sign a contract with a third-party payment institution to ensure business continuity.[99]

Another area of concern is information transparency and conflicts of interest in the process of selecting which loans to offer to customers. In some countries, P2P schemes have proved a fertile ground for fraudulent schemes long prohibited in traditional banking. The failure of a large P2P firm in China in 2016, Ezubao, affected almost 1 million customers, with losses exceeding $9.2 billion.[100] Three years later, another wave of failures affected over 380 P2P platforms in that country.[101]

In the US, a different incident involving its largest P2P platform was detected by the Federal Trade Commission – the nonfinancial consumer protection watchdog – which charged the platform “with falsely promising consumers they would receive a loan with ‘no hidden fees,’ when, in actuality, the company deducted hundreds or even thousands of dollars in hidden upfront fees from the loans”.[102]

Understandably, these events have led to strengthening regulations and supervisory policies in China, the US and elsewhere.

The FCA noted that information manipulation prompted by conflicts of interest can take subtle forms and listed the following schemes it has seen:

- “opaque fee arrangements between borrowers and the platform
- group structures that generate additional and invisible layers of earnings for the platform itself. For example, a company within the same group as a platform prefunds loans and sells them to the platform via novation, but the group company retains a stake in each loan and the price of the loan is set at a higher rate of interest than that received by retail investors
- platforms that allow staff or family members to transact on the secondary market, creating a risk that they have access to information that is not available to all investors which may benefit them (…)

98/ FCA. Loan-based (‘peer-to-peer’) and investment-based crowdfunding platforms: Feedback on our post-implementation review and proposed changes to the regulatory framework. July 2018.

99/ France. Ordinance No 2014-559 relating to crowdfunding. May 2014.

100/ Reuters. Leader of China's $9 billion Ezubao online scam gets life; 26 jailed. September 2017.

101/ Associated Press. China seizes $1.5 billion in online lending crackdown. February 2019.

102/ FTC. FTC Charges Lending Club with Deceiving Consumers. April 2018.

- platforms (sometimes through parent companies) that hold ‘skin in the game’ (i.e. they buy a part of the loans they help originate). Even though this can lead to a better standard of due diligence, it can also lead to conflicts of interest if they are able to use the secondary market to sell out early (possibly based on greater access to information), rather than holding to maturity

- platforms whose directors have presented loans for connected businesses but have not declared these connections to investors

- the transfer of loans from one client to another at an inappropriate price”.[103]

It should be noted that the FCA and many other authorities allow and even encourage P2P providers to participate in the loans offered to customers; the European Union in its proposed incoming P2P regulation forbids it. Authorities have also sought to constrain P2P providers from catering to a specific segment of the market, either investors and borrowers.

With few exceptions, P2P regulations set a high maximum amount for originated loans, expressing the authorities’ preference to direct this product to finance SMEs. The ceiling varies widely among jurisdictions but does not exceed US$ 6 million.

On the other side of the transaction, the FCA proposes introducing marketing restrictions that would limit direct financial promotions to investors who:

- “are certified or self-certify as sophisticated investors;
- are certified as high net worth investors;
- confirm before receiving a specific promotion that they will receive regulated investment advice or investment management services from an authorized person; or
- certify that they will not invest more than 10% of their net investible portfolio in P2P agreements”.[104]

The FCA recognizes that this restriction would force a drastic change in the target group for many P2P platforms, although it would align the UK regulation with the current regulation in the US, which largely is the same as the one applied to investments.

Regarding equity crowdfunding practices, most authorities recognize that this Fintech product is inherently riskier than P2P lending and other types of collective financing. At the same time, the retrenchment by banks from providing financing to SMEs as well as an increasing risk awareness among traditional sources of funding for start-ups following the 2008-09 global financial crisis has created a “growth capital gap”.[105] Authorities, therefore, are looking for innovative financing mechanisms to restore funding for these sectors. Equity crowdfunding is seen as a potential complement to other initiatives. For example, in the US, “the Jumpstart Our Business Startups (JOBS) Act created an exemption under the federal securities laws so that crowdfunding can be used to offer and sell securities to the general public”.[106] Similar government initiatives have taken place in Europe, Australia and Japan.

The regulation of equity crowdfunding is generally equivalent to that applied to retail investment, with relaxed requirements to allow for start-ups and unlisted companies to raise capital through these platforms. The product is subject to the same rules as other securities firms regarding the disclosure of the issuing firm’s financial conditions, main risks, the handling of client money, the requirement that investors must have investment experience and the platform’s conflicts of interest and risk management.

103/ FCA (July 2008).
104/ Idem.
105/ OECD. New Approaches to SME and Entrepreneurship Financing: Broadening the Range of Instruments. February 2015.
106/ US Securities and Exchanges Commission. Spotlight on Crowdfunding. February 2019.

3. CRYPTOASSETS

Financial authorities' practices regarding cryptoassets, as mentioned before, have been highly divergent, even taking opposing views in some respects. Moreover, authorities even use different words to identify these practices. "Some of the terms used by countries to reference cryptocurrency include digital currency (Argentina, Thailand, and Australia), virtual commodity (Canada, China, Taiwan), crypto-token (Germany), payment token (Switzerland), cyber currency (Italy and Lebanon), electronic currency (Colombia and Lebanon), and virtual asset (Honduras and Mexico)".[107]

This lack of a common term was reflected even within a single Fintech document[108] from the BCBS, where 'virtual cryptocurrencies', 'digital cryptocurrencies', and 'cryptocurrencies' refer to the same asset class. A year later, the BCBS opted to instead use 'cryptoassets', reflecting its "view that such assets do not reliably provide the standard functions of money and are unsafe to rely on as a medium of exchange or store of value".[109]

This discrepancy reflects the novelty of the products, a lack of clarity regarding their nature, the initial reluctance of the individuals and firms involved in cryptoassets to communicate with authorities and the hesitancy of regulated financial institutions to engage with anything labeled crypto.

While the transactions in cryptoassets remained insignificant and restricted to a small group of individuals, authorities judged that any action regarding cryptoassets did not merit their attention. It should be remembered that the first cryptoasset, Bitcoin, appeared ten years ago, just as the global financial crisis was demanding the attention of supervisors worldwide.

It was only in 2013, when a sustained and accelerated increase in the value of cryptoassets started to entice buyers beyond the initial group of committed individuals, that authorities started to look into this new world.

The first steps were tentative and oriented toward stopping the use of cryptoassets as a mechanism to circumvent AML/CFT regulations and financial sanctions. The AML/CFT enforcement authority in the United States, FinCEN, declared that "an administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations".[110]

Since this initial supervisory action, many jurisdictions have issued regulations or policy statements or have carried out enforcement actions regarding cryptoassets, its intermediaries or users. A compilation of cryptoasset regulations covering 130 jurisdictions by the US Library of Congress, provides a useful resource to identify practices on this topic.

That report and direct confirmation on authorities' websites reveal some common trends. Following discussions in late 2017, the G20's central banks started to issue similarly worded statements, which were rapidly echoed by other countries in a rare example of policy convergence on cryptoassets. These statements thus qualify as a general practice.

> Most jurisdictions warn their citizens that cryptoassets are not legal tender, are not backed by any authority or financial institution and are highly speculative investments.

107/ US Library of the Congress. Regulation of Cryptocurrency Around the World. June 2018.

108/ BCBS. Sound practices: Implications of Fintech developments for banks and bank supervisors. February 2018.

109/ BCBS. Statement on crypto-assets. March 2019.

110/ FinCEN. Guidance FIN-2013-G0001. March 2013.

Beyond the last statement, practices diverge sharply, as the following table shows:

TABLE 3: CRYPTOASSET REGULATION AND SUPERVISION CONTRASTING PRACTICES

Use of cryptoassets by the general public in transactions or as an investment	Prohibited: Ecuador, Bolivia, Algeria, Egypt	Explicitly allowed: Switzerland (some cantons), Malta, Gibraltar
Use of cryptoassets by financial institutions	Prohibited: India, Pakistan, Nepal	Explicitly allowed: Mexico, Japan, Isle of Man
Initial coin offerings	Banned: China, Pakistan	Regulated as securities offerings: Switzerland, USA, Gibraltar, Canada
Cryptoassets exchanges	Banned: China, Namibia	Regulated or registered by financial supervisor: Japan, South Korea, Australia, Philippines

Source: US Library of the Congress (2018) and information gathered by the author.

This table shows the extreme ends of the range of practices in representative jurisdictions. For each area, there are a range of practices between those extreme positions. As with other Fintech products, this is a rapidly evolving topic, which is likely to become more complex as central banks launch their own digital currencies. The US Library of Congress lists five jurisdictions, including two within ASBA membership,[111] that have launched or are testing national digital currencies.

A topic related to cryptoassets is the technology underpinning most of them: distributed ledger technology (DLT). Many financial institutions, central banks and other financial authorities are actively looking into the potential uses of DLT to make financial transactions cheaper and more secure. However, there is scant evidence of regulations or supervisory practices regarding DLT, partly because there are very few financial services or products using that technology. Only two jurisdictions have specific DLT regulations, Gibraltar and Malta.

The Gibraltar Financial Services Commission (GFSC) regulated "the use of distributed ledger technology by way of business for storing or transmitting value belonging to others to be regulated as a controlled activity under the Financial Services (Investment and Fiduciary Services) Act".[112] The norm creates a new type of licensed financial services firm, the DLT provider, and spells out nine regulatory principles that DLT providers must adhere to, mostly replicating high-level principles for managing financial institutions.

Malta, on the other hand, took a totally different approach. The country passed two laws: one creates the Malta Digital Innovation Authority[113] as the organization in charge of licensing, regulating and supervising the 'innovative technology services providers', which are defined by the second law.[114] Although both laws focus on DLT and related technologies, such as smart contracts, other new technologies can be included. It should be noted that there are no references to financial services in either law, apart from a requirement to coordinate with the Malta Financial Services Authority and other authorities on issues beyond the merely technological.

111/ The East Caribbean Central Bank and the Venezuelan government.

112/ GFSC. Financial Services (Distributed Ledger Technology Providers) Regulations. October 2017.

113/ Malta Parliament. Malta Digital Innovation Authority Act. July 2018.

114/ Malta Parliament. Innovative Technology Arrangements and Services Act. November 2018.

4. VIRTUAL BANKING

This type of financial institution (FTP-12) is "defined as a bank which primarily delivers retail banking services through the internet or other forms of electronic channels instead of physical branches"[115] by the HKMA.

As a financial institution allowed to engage in the whole range of activities, as any other standard bank, in principle, it should be regulated and supervised as such. In fact, most traditional banks provide a significant proportion of their retail services through electronic channels, and most regulations already provide for this delivery channel.

Nevertheless, a small number of authorities have opted to adapt their regulations and supervisory approaches to address issues exclusive to virtual banking. In all three jurisdictions with specific virtual bank practices – Hong Kong, South Korea and the European Union – the justification has been to encourage the authorization of new competitors in their markets.

Therefore, the regulations and supervisory policies relate mostly to the initial authorization process. In the cases of Hong Kong and South Korea, the regulators have aimed the flexibilization of the licensing process at removing barriers for nonfinancial companies to become significant shareholders in new virtual banks. In the case of South Korea, a new law[116] enables nonfinancial companies to own up to 34% of an internet-only bank instead of the standard maximum of 4%. The HKMA also relaxed the standard policy requirement that only banks can own over 50% of the capital of a bank incorporated in Hong Kong, accepting that nonfinancial firms may own virtual banks, albeit through an intermediate holding company incorporated in Hong Kong.[117]

The European Central Bank (ECB) accepts a wider range of possible shareholders in 'Fintech banks': "new Fintech subsidiaries of existing authorised banks; new market participants that adopt technological innovation to compete with established banks (…) [and] existing financial service providers (e.g. payment institutions, investment firms, electronic money institutions, etc.) that extend their scope to include banking activities and can therefore be considered new market entrants requiring a banking license.[118]

Both the HKMA and Korea's Financial Services Commission (KFSC) identify telecommunications companies as the most likely candidates to apply for virtual bank licenses. In the case of Korea, two such companies already have small stakes in banks.

In their policy statements, these authorities see these new financial institutions competing with established banks in the retail market.

The KFSC expects virtual banks to develop loan products targeted at people with average credit using a big-data-based credit rating system, provide easy mobile remittances using smart phones and accept loan applications without the submission of documents, among other retail customer-oriented features.[119]

Similarly, the HKMA envisages that "virtual banks should play an active role in promoting financial inclusion in delivering their banking services. While virtual banks are not expected to maintain physical branches, they should endeavour to take care of the needs of their target customers, be they individuals or SMEs. Virtual banks should not impose any minimum account balance requirement or low-balance fees on their customers".[120]

An area in common in these jurisdictions' approaches to licensing virtual banks is to require relevant technological knowledge by the management and board members to enable them to understand the risks that the business model requires.

115/ HKMA. Banking Ordinance Authorization of Virtual Banks. June 2018.

116/ National Law Information Center. Act on Special Cases Concerning the Establishment of Internet-Only Banks. 2019.

117/ HKMA (2018).

118/ ECB. Guide to assessments of Fintech credit institution licence applications. March 2018.

119/ Global Legal Insights. Banking Regulation 2019 – Korea. March 2019.

120/ HKMA (2018).

A concern shared by the HKMA and the ECB is that virtual banks could engage in an aggressive drive to obtain market share, which could lead to riskier activities. Additionally, these authorities feel that these new banks could face unexpected risks and difficulties in raising additional capital if needed. Therefore, both authorities are demanding exit plans.

> As virtual banks are subject to untested competitive challenges and unknown risks associated with the nature of their business models, in addition to the license application, the applicant should prepare an exit plan in case its business model turns out to be unsuccessful.

Once granted authorization, the three authorities estipulate that virtual banks will be subject to the same set of regulations as standard banks, including the relevant customer protection framework.

> The lack of a physical presence and virtual banks' reliance on electronic delivery channels must not affect their customers' rights to be treated fairly. Therefore, complaints must be handled through the same channels, and customers must be made aware of their responsibilities to maintain security in the use of virtual banking services and their potential liability if they do not.

IV. PRACTICES REGARDING FINTECH ENABLING TECHNOLOGIES

In the previous sections, this report examined practices regarding representative Fintech products and the Fintech landscape. This section surveys the financial authorities' actions regarding specific technologies associated with Fintech products.

It is evident from the review that supervisors are still trying to define a strategy regarding these technologies. In some cases, the practice has been to try to fit the treatment of these technologies into the existing set of regulations and policies, while, in others, a more restrictive approach has been implemented.

This ambivalence reflects the need to understand the effects that these technologies have on financial institutions' ability to remain sound and effectively manage their risks.

Finally, supervisors are examining how to harness the emerging technologies to improve their capabilities, the so-called 'RegTech' and 'SupTech', which is an interesting topic that is beyond the scope of this document.

1. CLOUD-BASED SERVICES

Financial institutions, as in many other industries, have embraced the benefits of transferring data storage, information processing and even the provision of services to third parties, providing those services through servers located remotely. The initial reaction of many supervisors was to treat these arrangements as any other outsourcing contract.

However, some authorities saw the need for specific policies and guidance as the reliance by financial institutions grew exponentially. The Bank of Israel was one of the first to issue a specific policy on cloud computing in 2015. It restricted the ability of regulated financial institutions to use those services, prohibiting the "use of cloud computing services for core activities and/or core systems"[121] and requiring prior approval from the supervisor to use other cloud-computing services, even when it did not involve customer data.

121/ Bank of Israel. Risk management in a cloud computing environment. June 2015.

Two years later, the Bank of Israel started to relax the initial set of restrictions, allowing banks to use certain cloud services without prior approval when four conditions were met:

a) "The cloud-computing application includes information that the banking corporation defines as sensitive.

b) The banking corporation does not define the information as sensitive; however, the disclosure of information can be used to deduce certain details that will enable to attack or harm the banking corporation and/or its customers.

c) Disruption or interruption of activity of the cloud-computing application may impair the conduct of the banking corporation and/or its ability to serve and respond to its customers.

d) The cloud-computing application provides cyber defense and information security measures as the only layer of protection, with no similar types of measures existing on the premises of the banking corporation".[122]

Then, in late 2018, the supervisor indicated that "in view of this and the accumulated experience, and similar to the directives issued by parallel supervisory authorities around the world, the new directive/amendment makes it easier for the banking corporations by cancelling the need to request a permit in advance from the Banking Supervision Department before implementing cloud technology, for certain applications such as storing the banking corporation's and/or customer's sensitive information on the cloud".[123] However, the prohibition on core systems remains in place.

In parallel, the European Banking Authority published a report[124] on cloud services, harmonizing the divergent approaches taken by national supervisors in this matter.

The document contains 7 recommendations:

- Materiality assessment, specifying that prior to engaging with a cloud services provider, the financial institution must assess the criticality of the data or processes outsourced;
- Duty to adequately inform supervisors, providing the authority with the information needed to adequately evaluate the suitability of the provider and contractual arrangements;
- Access and audit rights, allowing the financial institution and its supervisor access to the provider's premises, directly or by specialized third parties;
- Security of data and systems, setting the obligations of the provider to ensure the protection of the data received;
- Location of data and data processing, including within the risk management process the incidence of the political, data privacy and security risks of the provider's jurisdiction;
- Chain outsourcing, specifying the rationale for outsourcing to subcontract elements of the service to other providers and the additional risks involved; and
- Contingency plans and exit strategies, properly documented by the financial institution.

The Australian Prudential Regulation Authority (APRA), on the other hand, recently updated its guidance on cloud computing, indicating that "for arrangements with low inherent risk not involving off-shoring, APRA would not expect an APRA-regulated entity to consult with APRA prior to entering into the arrangement".[125]

122/ Bank of Israel. Directive 362—Cloud Computing. July 2017.

123/ Bank of Israel. The Banking Supervision Department is making it easier for the banks to use public cloud technology. November 2018.

124/ EBA. Recommendations on outsourcing to cloud service providers. December 2017.

125/ APRA. Outsourcing Involving Cloud Computing Services. September 2018.

In Latin America and the Caribbean, regulators have also included explicit requirements and limits on the use of cloud services within the operational risk management framework. Chile's supervisor, for example, developed a special chapter in its outsourcing regulations for cloud services, stating that, when using cloud providers for critical services, the regulated institutions must carry out a 'reinforced' due diligence of the provider. In those cases, the financial institution must ensure that the provider has internationally recognized certifications regarding security, business continuity and best practices. Additionally, there must be a legal opinion on privacy and data access in the jurisdiction of the cloud provider. The regulations mandate that the financial institution has a "contingency data processing centre located in Chile and demonstrate a recovery time compatible with the criticality of the outsourced service".[126] It is interesting to note that the jurisdiction of origin of any outsourcing firms, including cloud providers, must have an investment-grade country risk rating.

Similarly, the financial supervisor of Colombia recently issued a specific regulation for cloud services. The document defines mandatory risk management processes and minimum conditions for cloud services contracts. The supervisor also sets specific reporting requirements for these services and the documentation that financial institutions must have available for inspection. The authority also indicates that the financial institution must "establish the necessary measures to guarantee that, in the event of taking control, the [financial authorities], or whoever they designate, may access the information and the administration of the information systems that operate in the cloud".[127]

2. ARTIFICIAL INTELLIGENCE

Under this umbrella, a collection of related technologies has been increasingly tested and used to assist the decision-making processes in financial markets. However, as the FSB indicated in a report "because AI and machine learning applications are relatively new, there are no known dedicated international standards in this area".[128]

The few supervisory practices identified regarding the use of this technology in financial markets are in the securities market, specifically guidance on algorithmic models based on artificial intelligence by an US self-regulatory organization, the Financial Industry Regulatory Authority (FINRA)[129] and the European Union Directive on markets in financial instruments, known as MiFID II.[130]

In both cases, the emphasis is in the duty of regulated institutions to have "a robust development process in place (…) to ensure that possible risks are considered at every stage of the development process (…) in order to avoid market abuse and prevent the strategy from contributing to, or causing, disorderly market behaviour".[131]

There are other concerns regarding the use of this technology, such as built-in bias in credit analysis and banks following decision-making algorithms without a full understanding of the logical actions behind the process. However, there is no clarity regarding how to tackle these issues.

On the other hand, supervisors are looking positively toward developments that could simplify compliance by the regulated community and to support their own activities as part of the previously mentioned RegTech and SupTech.

126/ Superintendencia de Bancos e Instituciones Financieras Chile. Recopilación actualizada de normas. Capítulo 20-7. 2018.

127/ Superintendencia Financiera de Colombia. Instrucciones relacionadas con el uso de servicios de computación en la nube. March 2019.

128/ FSB. Artificial intelligence and machine learning in financial services. November 2017.

129/ Finra. Rule 3110. Supervision. June 2015.

130/ EU. Directive 2014/65/EU. May 2014.

131/ FSB (2017).

3. BIOMETRIC USER IDENTIFICATION

The increasing threat of financial fraud by using stolen identification credentials has prompted the development of diverse techniques ensuring that a person remotely accessing a financial institution is the legitimate owner of the account. Among the relevant emerging technologies, biometric identification[132] has been increasingly incorporated into so-called multifactor authentication.

There are few identified supervisory practices regarding the use of biometrics in financial markets. The most remarkable initiative, for its size and impact on financial inclusion, is the requirement by the Reserve Bank of India that "banks to ensure that all new card acceptance infrastructure deployed with effect from January 1, 2017 are enabled for processing payment transactions using Aadhaar-based biometric authentication".[133] Aadhaar is a national identification scheme that incorporates fingerprints to authenticate the person. Although, following a Supreme Court ruling, it is not mandatory for individuals to have the Aadhaar ID to open a bank account, the supervisor decision has ensured that the payment system is ready to secure transactions using biometric identification.

The other case of a supervisor mandating biometric identification is a ruling by the New York State Department of Financial Services on cybersecurity, which requires regulated financial institutions to provide multifactor authentication, including "inherence factors, such as a biometric characteristic".[134]

It should be noted that Mexico's CNBV prescribed mandatory biometric technology to identify financial users within the cybersecurity regulations mentioned in section II.8. The regulation stipulates that financial institutions, including the new financial technology institutions, must implement biometric identification by March 2020.

The regulation also specifies that while biometric identification has not been implemented, "in the event that its clients file claims [for fraud] (…) carried out by third parties claiming to be the client in question, they undertake to assume the risks and, therefore, the amounts of these claims. (…) The respective amounts will be paid, no later than twenty days after the filing of the claim".[135] This regulation undoubtedly incentivizes financial institutions to implement biometric identification well before the official deadline.

Another interesting provision is that "prior to the capture of the (…) biometric data of its users, the institutions must capture the same biometric data of their employees, managers and officials in charge of this function, and verify that the biometric data of the clients do not correspond with those of said employees, managers and officials".[136]

132/ Understood as individual characteristics inherent to a specific person.

133/ Reserve Bank of India. Aadhaar-based Authentication for Card Present Transactions. September 2016.

134/ New York State Department of Financial Services. Cybersecurity Requirements for Financial Services Companies. March 2017.

135/ CNBV. Disposiciones de carácter general aplicables a las instituciones de crédito. Reformed in November 2018.

136/ Idem.

V. CONCLUDING REMARKS

As was mentioned several times throughout this report, regulatory and supervisory practices are evolving continuously, in part as a result of new evidence and greater understanding by the authorities of the risks and benefits of Fintech products and their associated technologies.

There are some topics that are relevant to financial services that this report does not address, such as data privacy, as their regulation is usually outside the scope of financial authorities.

Additionally, as was mentioned above, developments in Fintech that are of interest with regard to the authorities' own activities were excluded from consideration, as they are outside the scope of this document an interesting topic that is beyond the scope of this document.

ANNEX 1

JURISDICTIONS REVIEWED

Name	Continent	Name	Continent
Argentina	America	Denmark	Europe
Barbados	America	Finland	Europe
Bolivia	America	France	Europe
Brazil	America	Germany	Europe
Canada	America	Gibraltar	Europe
Chile	America	Hungary	Europe
Colombia	America	Iceland	Europe
Ecuador	America	Ireland	Europe
Mexico	America	Isle of Man	Europe
Peru	America	Italy	Europe
USA	America	Lithuania	Europe
China	Asia	Luxembourg	Europe
Dubai	Asia	Malta	Europe
Hong Kong	Asia	Netherlands	Europe
India	Asia	Norway	Europe
Indonesia	Asia	Poland	Europe
Israel	Asia	Portugal	Europe
Japan	Asia	Russia	Europe
Korea	Asia	Spain	Europe
Malaysia	Asia	Sweden	Europe
Philippines	Asia	Switzerland	Europe
Singapore	Asia	Ukraine	Europe
Taiwan	Asia	United Kingdom	Europe
Turkey	Asia	Botswana	Africa
Australia	Oceania	Cameroon	Africa
New Zealand	Oceania	Ghana	Africa
		Kenya	Africa
		Nigeria	Africa
		South Africa	Africa
		Tanzania	Africa

ANNEX 2

OBSERVED FINTECH PROMOTION SCHEMES BY FINANCIAL AUTHORITIES

Jurisdiction	Dedicated Unit/ Channel	Innovation Hub	Regulatory Sandbox	Special Fintech License
Denmark	X	X	X	
Finland	X	X		
France	X	X		
Italy	X			
Malta	X	X	X	
Netherlands	X	X	X	
Poland	X	X	X	
Portugal	X	X		
Lithuania	X	X	X	X
Sweden		X		
United Kingdom	X	X	X	
Spain	X		X	
Switzerland	X	X	X	X
Isle of Man	X	X	X	
Australia		X	X	
New Zealand	X			
Dubai	X	X	X	X
Singapore	X	X	X	
Japan	X	X		
Korea	X		X	X
Malaysia	X	X	X	
India			X	
Indonesia	X		X	X
Hong Kong	X	X	X	X
Taiwan	X	X	X	
South Africa	X			
USA	X		X	
Brazil				X
Mexico		X	X	X
Argentina	X	X		
Barbados	X		X	
Colombia	X	X	X	X
Total	**27**	**22**	**22**	**9**

ANNEX 3

OBSERVED FINTECH LICENSING SCHEMES BREAKDOWN BY JURISDICTION

Jurisdiction	Payment	P2P	Crowdfunding	Cryptoassets	Virtual bank
Denmark	X				
Finland	X		X		
France	X	X	X		
Germany	X		X		
Hungary	X				
Ireland	X				
Italy	X		X		
Luxembourg	X				
Lithuania	X	X			
Malta	X				
Netherlands	X	X			
Poland	X				
Portugal	X		X		
Sweden	X				
United Kingdom	X				
Spain	X	X	X		
Iceland	X				
Norway	X				
Switzerland			X		
Gibraltar	X			X	
Isle of Man	X	X	X		
Dubai	X	X	X		
New Zealand		X	X		
Singapore	X				
Japan	X			X	
Korea	X				X
Malaysia	X	X	X		X
India	X	X			
Indonesia	X	X			
Philippines	X				
China	X	X	X		
Hong Kong	X				X
Taiwan	X				

ANNEX 3

OBSERVED FINTECH LICENSING SCHEMES BREAKDOWN BY JURISDICTION

Jurisdiction	Payment	P2P	Crowdfunding	Cryptoassets	Virtual bank
Cameroon	X				
Ghana	X				
Kenya	X				
Nigeria	X				
Tanzania	X				
Canada	X	X	X		
USA	X		X	X	
Colombia	X		X		
Brazil		X	X		
Mexico	X	X	X		
Chile	X				
Peru	X				
Ecuador	X				
Bolivia	X				
Total	**44**	**14**	**17**	**3**	**3**

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

ASBA MEMBERS

Associate Members

Andean Region

Superintendencia Financiera de Colombia
Superintendencia de las Instituciones del Sector Bancario, Venezuela
Autoridad de Supervisión del Sistema Financiero, Bolivia
Superintendencia de Bancos del Ecuador
Superintendencia de Banca, Seguros y AFP, Perú

Caribbean Region

Central Bank of Belize
Oficina del Comisionado de Instituciones Financieras, Puerto Rico
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

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

GLOBAL FINTECH REGULATION AND SUPERVISION PRACTICES

Executing Agency: Association of Supervisors of Banks of the Americas (ASBA)

Financed by: IDB Lab

Project: Regulation for Responsible and Competitive Financial Sector Innovation

Technical Cooperation: ATN/ME-15724-RG

December 2019.

For additional information: asba@asbasupervision.org

C. Picacho Ajusco #238, Of. 601

Col. Jardines en la Montaña, C.P. 14210

Mexico City, Mexico

(5255) 5662-0085