ASBA
ASSOCIATION OF SUPERVISORS OF BANKS OF THE AMERICAS

Financial Stability Institute
BANK FOR INTERNATIONAL SETTLEMENTS

Highlights of the

Policy Implementation Meeting on Fintech and Cyber Risk

Montevideo, Uruguay, November 14 and 15, 2018

Contents

Introduction 3

Technologies and common challenges 4

Public Sector 5

Private Sector 7

Introduction

The Association of Bank Supervisors of the Americas (ASBA) and the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS) organized a Policy Implementation Meeting (PIM) on Fintech and Cyber Risk in Montevideo, Uruguay on November 14 and 15, 2018. The meeting's objective was to assess the current fintech environment and the critical challenges that cybersecurity poses to banks and regulators in the context of enhanced digitalization of the banking business.

Both supervisors from ASBA member jurisdictions and select overseas countries as well as private sector experts gained greater knowledge about the evolution of new technologies, their application in finance, their integration in regulatory and supervisory frameworks, and their potential impact on the soundness and safety of the financial sector. The meeting sought to increase the supervisors' understanding of these critical developments impacting the financial landscape of the Americas in an active dialogue. This meeting sowed the seeds for a continued discussion in another PIM planned to be held in Mexico City on June 26 and 27, 2019.

The meeting comprised six sessions addressing both opportunities and challenges stemming from the use of new technologies in the financial sector as well as their potential impacts on banks and supervisory approaches. The discussion reflected both perspectives from the private and the public sector.

The first session presented the private sector's perspective, in which banks and other market participants discussed the current development of fintech and the related challenges that it presents to financial intermediation. The second session elaborated on current cybersecurity threats to financial institutions and the strategies being developed to counter them. The third session concentrated on the entry of new fintech competitors and the use of enhanced technologies in the financial sector. In particular, it focused on the analysis of new and changing business models, including risk management practices in banks mainly driven by fintech developments.

The fourth session provided a general overview of the potential use of technologies in supervisory activities, typically called "suptech" applications. These are still at an early stage, though participants had an opportunity to learn about a range of applications and solutions under development or those that may become operational in the short term.

The fifth and sixth sessions addressed the public sector's perspective on two issues. The first examined fintech implications for regulation and supervision. A significant challenge that various jurisdictions face is the development of a proportional framework balancing prudence and innovation while securing a level playing field for existing players and new entrants. The second issue looked at the strategies that the public sector is adopting to deal with cyber risk in the region.

The following section presents a summary of the experiences shared by the participants as well as the most relevant findings and conclusions of the meeting.

Technologies and common challenges

The group identified technologies based on their characteristics and potential for disrupting financial institutions and the public sector. Potential benefits of the new technologies supporting market efficiency, furthering current business models in banks, promoting financial inclusion, and supporting regulatory and supervisory activities were discussed. The following were the most disruptive technologies identified:

- Open Banking. The use of APIs (Application Programming Interfaces) to allow third parties to access financial institutions' customer data and other general information for the development of products and services.
- Cloud computing. This is an information technology model that consists of the provision and use of configurable on-demand computing resources (e.g., servers, storage, applications, and more) via an internet network, as opposed to a physical connection to a local server. Cloud computing services enable customers to store information, processes, and data on servers that may be accessed through any computer with an internet connection[1].
- Blockchain. Although mostly known for its use in the development of cryptocurrencies, this technology has other relevant applications in the financial sector, for example, insurance and contract management. To date, the technology has not penetrated extensively in the financial sector; however, it is under scrutiny by the public and private sector due to its possible implications for the introduction of market frictions, customer identification, and money laundering, among others.
- Cryptocurrencies. Blockchain and cryptocurrency are not synonyms. Some cryptocurrencies are based on different types of technologies. There is a difference in opinion on this matter; while some authorities and market participants promote the use of virtual currencies, governments and international organizations are highlighting the economic and social risks that these instruments could bring to the market. No consensus exists on the usefulness or repercussions of these technologies.
- Artificial Intelligence (AI). Currently, most AI models are used in the private sector: the use of *chatbots* for customer question and answer management and *machine learning* for tailoring services and credit ratings, among others. However, managed properly, this technology could support the public sector, especially in improving the efficiency of some supervisory activities.

Given the accelerated evolution and introduction of new technologies, regulators, supervisors and financial services providers are exposed to strategic and reputational risks. On the one hand, these risks could potentially impact the financial performance of institutions to the extent that their current decisions (changing the business models, associations and outsourcing) deviate from the inertia of the sector as a whole. Despite the increasing importance of reputational risk, the vast majority of firms do not seem to have a well-thought-out strategic approach to proper reputational risk management. Instead, reputational risk is typically approached as a crisis management issue, focusing primarily on the aftermath of an event. On the other hand, financial institutions' reputational deficiencies can indirectly challenge the credibility and competence of regulatory and supervisory authorities.

An important issue related to the strategic and reputational aspects is the increasing use of outsourcing services leading to potential vendor concentration. The increased use of third parties (technological solutions vendors, cloud-based products and others) imposes a further dimension of existing operational risk on the reputation of the outsourcing institution, which could be both a financial and a supervisory institution. The less the financial institutions and supervisors know about the third parties, the higher the risk. Harmful behavior of a third-party provider of services may ricochet and negatively affect the reputation of the institution and the supervisory agency,

[1] ASBA, An Overview of Fintechs: Their Benefits and Risks, 2017

especially as the public perceives them as protectors of the customer (even though in some countries this is not their mandate). The problem worsens when third-party providers offer their services to many institutions, including across borders.

Cybersecurity is an important problem that affects many economic sectors. However, the financial sector is more prone to this type of threat. The number and sophistication of cyber attacks on the financial sector have increased considerably over the past few years. In the private sector, the attacks come through significant withdrawals of money, fraud, identity theft, and more. The public sector is exposed to the stealing of sensitive information about the operations of the financial sector and the hindering of regulatory and supervisory activities. The increasing dependency on technologies and external providers amplifies the problem. Setting clear supervisory expectations about dealing with cyber risk and training the institutions as well as raising their awareness is critical. Additionally, bank customers and bank employees must understand their own crucial role in the prevention and reporting of cyber attacks.

Cybersecurity is an issue that should be treated in stages. In this sense, three important stages have been identified. The first stage is raising awareness and acknowledging the existence of the problem. This includes an understanding of where the attacks could come from, identifying the most vulnerable areas, and training staff (many of the attacks are successful because institutions' staff allow it, either voluntarily or involuntarily). The second stage is the development of a strategy and the tools to appropriately respond to and deal with a cyber attack. These include technological and policy tools as well as manuals to possibly prevent and counter an attack. It is essential that external providers should be part of the cyber resilience policies. The third and final stage is the implementation and making an effective use of the policies, manuals, and tools available. This is the most challenging stage, since it requires a collective effort and a possibly more radical change in the culture of the institutions.

The customer and his or her data have become critical elements of the new financial environment. Currently, there exists a perception that banks, other financial institutions, and fintechs are competing to provide a better experience for the customer. Thus, the customer has become the focus, and financial data and nonfinancial data (social media, locations, and more) have become more valuable for the design and provision of financial products and services.

Two fundamental matters were identified regarding the client and his or her data: symmetry in access to financial information and a lack of definition of public data and public interest data. First, related to the open banking issue, some jurisdictions have issued regulation to promote data sharing mechanisms, whereby banks will be obliged to provide access to some financial information on their clients. Experts mentioned that this issue has the potential to add strategic and reputational risks if implemented incorrectly. Second, from a public policy point of view, there is still a problem in defining the exact meaning of public data and public interest data. There is not much clarity beyond recognizing its importance. However, if a data profile is agreed upon, the development of mechanisms that may allow for formal and legal access to data will be critical.

Public Sector

The new environment may require a change in the mindset, culture, and procedures of the regulatory and supervisory agencies. Firstly, supervisory authorities need to develop new skill sets in their supervisory staff. Although, in general, the mandate and the responsibilities of the supervisors may not change in the face of this new environment, supervisors must build an additional and new supervisory profile and develop new skills and tools making use of the new technologies. In other words, public policy objectives may not change, but the procedures and the capabilities to deliver and manage them will change. The new supervisor's profile must be more forward-looking, proactive, able to use innovative technologies, and he or she must understand the macroeconomic aspects and traditional microprudential assessments of financial institutions.

Disruption of bank business models due to the entry of new technologies into the financial sector means that regulators and supervisors who are in charge of overseeing banks and traditional institutions will increasingly have to coordinate with and consider other stakeholders. This notion goes further than the idea of supervising fintechs. The growing interconnection with stakeholders in the financial system, the embedding of new technologies into the "traditional" regulated institutions, the development of an important area outside of regulation, and the interaction with specialized third-parties will directly or indirectly force the regulators and supervisors to oversee other stakeholders (e.g., payment platforms, cloud-solutions providers, and a range of different supporting APIs). This will bring them out of their comfort zone: from only supervising prudential and conduct issues to addressing concerns such as governance in a digitally led business environment, financial information management, sound open-banking arrangements, or cybersecurity threats management.

Regarding the use of innovation, the public sector has been trailing behind the private sector. The use of new technologies will be essential in future supervisory activities. The public sector has not had the same incentives as the private sector for investing in technological developments that can make their activities more efficient. The private sector has developed in such a way that it has begun to produce large amounts of information that the public sector has difficulties in managing. Some types of technologies that could help supervisors to carry out their functions are *big data* analysis and artificial intelligence tools.

The development of suptech solutions is a long-term investment, and it does not imply that supervisors may be replaced, though a more efficient use of supervisory resources is important. Indeed, some supervisory institutions have started to develop in-house or outsourced supporting tools for supervision; others have not begun this potential modernization process. The adoption of suptech approaches helps supervisors become more proactive and forward-looking. Additionally, strategies will have to be developed to attract and retain expert talent on the collection, integrity verification, analysis, and interpretation of information to respond to the challenges posed by the market on a timely basis.

Regulators and supervisors still lack clarity regarding setting the regulatory perimeter for actors and their activities. The public sector is facing a dilemma in finding the right balance to regulate or not to regulate some innovations. If the regulation begins too soon, there is the possibility of hampering beneficial innovations that could make the markets more competitive and efficient. On the other hand, if the time is too protracted, some inherent financial stability risks could arise without having the necessary regulatory and supervisory tools to contain them. This is particularly important in regard to systemic issues.

Some supervisors consider that financial innovation regulations should be developed in stages, addressing the most urgent issues through current (or slightly modified) regulatory and supervisory tools and developing new policy instruments as the market evolves. The first stage would be to work on building mechanisms that create the right incentives through existing regulations. Basic principles should be developed for products and financial services that deviate from the current incentives. Finally, in some cases, it may be necessary to adopt prescriptive rules when certain business models surpass the established principles and when the rules must be tighter for better control and management of the supervisor.

A principle-based regulation instead of prescriptive rules, such as that proposed by the UK's Financial Conduct Authority, may give flexibility to the responsible adoption of technological innovations in the financial sector in the first stages. There is still a debate about the advantages and disadvantages of principle-based and rule-based approaches. A principle-based approach could be suitable for the following reasons: providers know their business better than anyone else and there is a shortage of experts on information technology in public institutions, an inadequate understanding of the operation of the new technologies, and limited evidence for understanding the impact of certain technologies in the financial sector. In this context, coordination between regulators and the private sector is important in cases where the regulator sets the objectives, and the private sector could develop proposals on how to achieve these objectives. However, a rule-based approach cannot be dismissed in some

instances or activities as markets evolve. The combination of both methods may very well balance out the benefits and risks of financial innovation.

Discussion on the regulatory perimeter led to the notion that same risks should comply with the same regulation. While some jurisdictions focus on the underlying financial activity, others consider that regulating technology will be fundamental (e.g., cloud computing, APIs, blockchain). Nevertheless, there seems to be a tacit agreement that the same risks should comply with the same regulations, although this might be difficult to achieve in practice.

Undoubtedly, in this new environment, operational risk has grown and will continue growing. One of the most critical challenges, from a regulatory perspective, is to understand to what extent some issues could be considered within the existing operational risk management framework. From the BCBS point of view, operational risk management standards are still applicable to technological and cyber risk issues. On the other hand, banks and some regulators consider that technological issues must be addressed from a different perspective, though there is no clarity about the best approach. Some jurisdictions, such as Germany, have developed a broader methodology and cooperate with experts to oversee cybersecurity management frameworks within the financial institutions. Other jurisdictions, such as Chile, have adopted a less direct stance, addressing the problem from a more comprehensive perspective in communication with other authorities (e.g., through a National Strategy).

The regulator/supervisor must understand his or her role within the set of strategies that address technological and cybersecurity risks. Some activities transcend the usual financial activities and jurisdictional limits. Even though the financial sector is more prone to attacks, cyber risk transcends to other sectors and jurisdictions. On the one hand, the regulator must understand what both his or her role and scope are within the group of authorities that could have the same concerns and, from there on, develop an internal strategy that does not conflict with other authorities or mandates. On the other hand, certain products and services operate in more than one jurisdiction. Although there is no clear strategy on how to face the cross-border issue, communication among authorities of different countries and regions is essential.

Fintechs and other technological developments can support financial inclusion when combined with other policy mechanisms. A couple of years ago, there was the perception that the entry of fintechs was a synonym for financial inclusion. The current developments have shown that these innovations are also helpful in providing better financial services for well-served segments of the market. However, many fintechs are currently not considering the underserved or non-served segments in their strategies, leaving ample room to expand their business models.

Private Sector

Although tensions exist among nonregulated technological entities and regulated financial institutions, there seems to be a convergence to a more collaborative environment. The development of the fintech ecosystem is occurring more collaboratively than competitively compared to some years ago. The new stakeholders need the infrastructure and could benefit from the experience and confidence that current customers have in the traditional system. Additionally, financial institutions seem to be more explicit about the impact of fintech on their business strategies and either partner with new stakeholders or invest in digital strategies that can help them adapt to the new environment.

In the current context, decisions about digital strategies are taking place in an environment of significant regulatory changes. New players but also traditional financial institutions that incorporate these new technologies into their services are part of the ecosystem known as fintech. However, the recent finalization of the Basel III package and the intensive implementation process in progress pose an additional challenge to banks since they will have to balance their strategic priorities between regulatory compliance and digital innovations, among others. The above has added to the tension between banks and regulatory demands.

A proportional approach, although it is not clear what it may look like, could help, but it has limitations at times when defining the depth and scope of this process. The adoption of proportional regulatory and supervisory frameworks in a digital world is challenged by the reach of new technologies, their legal management complexities, and the insufficiency of some of the current legal frameworks.

The bargaining power between financial institutions and their customers is disturbed by the entry of new stakeholders. Until a few years ago, the bargaining power of banks over their clients was ample. The entry of new stakeholders has allowed customers to choose among other service options that are easier to use and have lower costs, even though they are not necessarily the safest. Today, the competition is in providing the customer with a friendly and personal experience; thus, traditional financial institutions are compelled to develop strategies to improve their clients' experience.

Both fintechs and traditional financial institutions must understand that the transformation of the financial sector is, to a large extent, centered on customers. The customers must be aware of their role and the value of their information. Financial service providers will increasingly depend on the access and use of customers' data. The inherent value of data becomes material. Nevertheless, customers are still unaware of the cost of their information and the strength of their bargaining power. When customers become aware of the value of their data, the dynamics of the market may shift because they will have under their control the decision of with whom, when and for what purposes they will share their information. In this sense, the current use of automatic tools and the lack of rules for new competitors represent security risks for customers.

The sharing of information will be fundamental in the new environment. However, some *open banking* structures could represent threats to the integrity of financial institutions. When entering into a sharing of information structure, banks will be able to access other markets or government APIs that will allow them to expand their services, introduce new solutions, and identify—with greater precision—the changes in the information of their clients. Conversely, there could be some mismatches when accessing information because when a bank opens its APIs, it will allow fintechs and other stakeholders to access sensitive client data. This access is not necessarily detrimental; however, in some schemes, a client may authorize the use of his or her data by a third party that has no relationship with the bank. Thus, if the access results in a conflict, the responsibility and reputational risk will fall on the bank. Although there are private (such as in the USA) and public (PSD2 in Europe) initiatives, the impacts and benefits of the emerging information access initiatives are not clear.

The entry of large technological companies (Big Tech) into the provision of financial services could bring about important challenges concerning competition and systemic risk and may impact banking business along different dimensions. It is reasonable to think that large companies dominating the technology market may also want to provide financial services. Their comparative advantage lies in the existing client relationships, including customer data availability, and in being able to develop the required IT platforms and infrastructure for the provision of financial services. Conversely, they might be shy about accepting the cost and the additional burden of regulatory compliance associated with receiving a banking license. If Big Tech enter the market, there could be an obvious risk of market concentration and competitive tensions with the traditional banking system. Moreover, their international presence has the potential to bring about systemic risks. Additionally, if the Big Tech companies become third parties providing services to the financial sector, there are obvious concerns about technological dependence and risk concentration.