CONSUMER PROTECTION IN THE NEW ENVIRONMENT OF FINANCIAL TECHNOLOGICAL INNOVATION

REGULATORY AND SUPERVISORY CONSIDERATIONS

Regulation for Responsible and Competitive Financial Sector Innovation

June 2020

ASBA

IDB | LAB

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

For additional information: asba@asbasupervision.org

asbasupervision.com

T. (5255) 5662-0085

Design by Tinta Roja Editoras, contacto@tintarojaeditoras.com

ACKNOWLEDGEMENTS

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

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

CONTENTS

INTRODUCTION

Fintech developments have introduced the use of innovative technologies in the provision of banking services, reshaping the business models, channels, services and market competition of the financial industry, as well as creating new risks. Under this new unprecedented disruptive scheme, the Association of Supervisors of Banks of the Americas (ASBA), with support from the Inter-American Development Bank (IDB), formed a Working Group (WG)[1] under the leadership of an expert consultant,[2] with the objective of establishing minimum guidelines and regulatory recommendations for the incorporation of innovative technologies in the financial sector in a responsible, transparent and competitive manner. To fulfill the goal, the Association decided to analyze the ecosystem of technological financial products (fintech) from the prudential and non-prudential approaches.

This document focuses on the non-prudential analysis of fintech's regulation and supervision. To develop the regulatory and supervisory guidelines, a study on marketing practices, information disclosure and transparency was conducted, from which good practices and opportunities for improvement were identified, always considering the protection of the user of the identified products or services as a reference point. By reviewing the information collected, the experience identified in other jurisdictions, the advice of the WG and the ASBA technical team, the document compiles those proposals for minimum regulatory and supervisory considerations that are applicable to all fintech products and services in the region.

Based on the analysis conducted, it is possible to establish minimum guidelines and recommendations based on common regulatory and supervisory initiatives and trends for consumer protection. These will be developed throughout the document considering three fundamental aspects.

First, **regulation should be neutral** towards technological change and business models and should neither encourage nor hinder them. Rather, regulation should allow for fair competition between all market players, i.e., analog versus digital; existing versus new, highly digital business models; local versus expanding foreign competitors. The above should be without prejudice to the duty of the Regulatory and Supervisory Authorities (RSAs) to know and analyze technological developments in order to assess their potential, among others in the face of financial inclusion initiatives, as well as the risks that such developments may pose.

1 We appreciate the participation of the Working Group integrated by the following ASBA member institutions: Autoridad de Supervisión del Sistema Financiero (Bolivia), Banco Central Do Brasil (Brazil), Comisión para el Mercado Financiero (Chile), Superintendencia General de Entidades Financieras (Costa Rica), Banco de España (Spain), Superintendencia de Banca, Seguros y AFP (Peru).

2 Roberto Borrás is a Colombian lawyer, advisor on financial regulatory matters and a partner of Garrigues since 2015. He was the Financial Superintendent of Colombia, Director General of Financial Regulation at the Ministry of Finance and Public Credit (currently URF) and Chairman of the Colombian Securities Market Self-Regulator. He was also Deputy Superintendent of Risks and Superintendent of Corporate Conglomerates at the Financial Superintendence of Colombia. Among other positions he was advisor to the National Government in the preparation of the Financial Inclusion Bill (1735 of 2014) by means of which the SEDPES were created. He has been a consultant for the World Bank and the Inter-American Development Bank.

Second, **regulation should be based on principles**. Jurisdictions at the forefront of developing the industry of digital financial products and service providers tend to apply such a regulatory approach because it is much more flexible in terms of its actual application to financial ventures as opposed to rule-based regulations, regardless of whether an analog or digital channel is chosen.

Principled-based regulation has been shown to provide room for innovation, as well as to recognize the accelerated changes in the provision of financial services, allowing for dynamic and effective application of the standards in a changing environment. In contrast, an over-prescriptive scheme, characterized by controlling everything down to the last detail, tends to stifle innovation.[3]

Third, it is essential to **prevent the emergence of regulatory gaps or arbitrage** caused by the appearance of new providers who, being outside the regulatory perimeter, carry out activities that are the same or structurally similar to those carried out by providers of traditional (incumbent) financial institutions.[4]

In this regard, it is relevant to consider that several incumbent entities in the region have been active in the development of fintech initiatives. These incumbents seek to optimize the provision of their services, by trying to reach more citizens in different places, regardless of their geographical area, by creating new channels, as well as proposing better operating conditions for the products, making them safer for the consumer and providing more competitive schemes. In general, developments by incumbents, as they are within the regulatory perimeter, have taken place with strict adherence to consumer protection regulations, either by attending to special rules for the financial industry or cross-cutting standards applicable to it.

It should be borne in mind that there is a close relationship between privacy guidelines in the financial sphere, the protection of personal data and adequate protection of the financial consumer. This is why it is clear that many of the issues dealt with in this document may involve activities and functions not only of financial supervisors and regulators, but also of the personal data supervisory institutions present in each jurisdiction.

Also, it is worth mentioning that financial RSAs should collaborate closely with these institutions to strengthen the dissemination of regulations and to be included in the financial projects of technological innovations. It should be noted that regional legislation on personal data protection shares the same philosophy and guidelines as the European General Data Protection Regulation (GDPR), which provides a broad legal basis on the subject.[5]

That said, this document is divided into eight sections. The first section describes the characteristics of digital consumers and some of their cross-cutting concerns. The second section sets out some preliminary considerations for developing effective strategies and actions that regulators can adopt for the adequate protection of the digital financial consumer. The third sets out general considerations and recommendations to ensure a fair environment by avoiding regulatory arbitrage between fintech and traditional financial institutions. The fourth sets out particular considerations and recommendations regarding the duties and rights of digital financial consumers. The fifth provides specific considerations for products or services that have been identified as having the greatest use and/or potential for use in the Americas. The sixth discusses alternatives for a supervisory model of consumer behavior and protection in the new technological environment (risk-based supervisory model and proven accountability model). The seventh examines considerations for the implementation of supervision strategies. Finally, the eighth section describes the upcoming challenges for regulators and supervisors and offers some final comments.

3 https://www.bbva.com/en/countries-leading-fintech-regulation/

4 Throughout this document, the term incumbent will be used to refer to those traditional financial institutions that stand in opposition to innovative financial providers.

5 https://gdpr-info.eu/

DIGITAL FINANCIAL CONSUMER PROTECTION CONCERNS

Digital innovations, the increased power of telecommunication networks and mobile devices, the widespread use of social networks, and cloud computing have created more sophisticated consumers.

Today consumers have tools to research, select and purchase digital products and services, but are less aware of their rights as consumers than those using traditional media. Some studies[6] show the following descriptions of digital financial consumers.

- They belong mostly to the so-called "millennial" generation (born between 1981 and 1993) because they are the first fully digital generation. These consumers show a greater dependence on digital platforms and adopt products and services with the newest digital features available on the market, increasingly at a faster pace and with the widest scope.
- They find it easier to "set up" an account with a mobile application from an unsupervised fintech provider than to use a tool or channel provided by a traditional financial institution (FI). While older generations prefer more personal interaction with their financial providers and tend to be suspicious of digital solutions, younger generations prefer not to visit a traditional FI, as they feel it is too time consuming and, moreover, do not trust these institutions after the financial crisis.
- They want to access the same variety of products and services in all channels (omnicanality), either through the website or through an application (*app*), and using a smartphone, tablet or computer without affecting the quality of service.
- They believe that new fintech service companies may have more attractive rates and fees for their services than traditional FIs.
- They expect 24/7 service because they think they can access more services and products while doing a day-to-day activity rather than just a specific service for which they must visit a branch. They also expect their requests and complaints to be resolved in a very short time, within hours or on the day of their complaint.
- They are convinced that innovative financial technology solutions provide a better online experience and functionality for their services compared to a traditional FI's website, and they intuitively become familiar with the features of fintech's apps, as the user experience is focused on getting results rather than providing a lot of information that they consider "unnecessary".
- They are willing to change the entity if another one offers better conditions. In addition, they will share any comments or complaints through social networks.
- They are at great risk of experiencing stress and embarking on bad financial management. In fact, those who use mobile payments are nearly 16 percentage points more likely to overdraw their checking accounts (than those who do not use mobile payments) and 23 percentage points closer

6 https://pdf4pro.com/cdn/millennials-and-wealth-management-inside-article-21c251.pdf; https://www.bbva.com/es/cliente-mas-exigente-consumidor-digital/; https://usa.visa.com/dam/VCOM/global/partner-with-us/documents/visa-new-digital-consumer.pdf

to accessing alternative financial services (pawn shops and day-to-day loans). Likewise, those who use mobile payments show lower levels of financial education and worse financial management practices than non-users.[7]

Under this environment, it is appropriate for RSAs to consider how financial consumers should be protected and whether the risks arising from digitization are adequately addressed in their current consumer protection processes and regulations.

On this point, the Bureau Européen des Unions de Consommateurs (BEUC) in response to the European Commission's public consultation on fintech has argued that from the consumer's point of view "it does not matter whether a bank, a non-bank payment service provider, a collective financing platform or an advisory robot provides a financial service; the consumer expects to be treated fairly (equally) at the pre-contractual, contractual and post-contractual stages, such as clear and non-deceptive advertising, an explanation of all possible risks related to the product and an efficient framework for resolving possible disputes."[8]

In this way, the digitalization of financial products and services can mean that digital financial consumers are also exposed to "new" risks (particularly when compared to traditional financial products), and it is especially important to understand the potential problems of innovation and digitalization from a consumer perspective. Below are some cross-cutting concerns regarding consumer protection.

Access to financial products and services

- Reduced access to financial products and services for consumers who lack digital skills, little financial education or little access to technology to operate in the digitalized financial services environment.
- Instant and/or simplified access to financial products and services can result in poor decision-making and potential financial disadvantage for the consumer.
- The unique use of digital consumer data to assess consumer creditworthiness can reduce the accuracy of credit evaluations and increase financial exclusion (exactly the opposite effect to the one desired).
- Difficulty in identifying and interacting with vulnerable consumers by businesses due to the loss of direct human interaction.
- Exclusion from certain personalized products and services because the consumer has not generated a fingerprint or sufficient personal data online or refuses to share his or her personal data.
- Customization of products can reduce critical thinking by consumers in the decision-making process.

Dissemination of Information and Counseling to Consumers

- Use of promotions and/or paid advertising about products or services online that are falsely presented as unbiased or independent.
- Use of social media marketing to inappropriately target consumers who do not have a full understanding of the risks associated with certain products and services, particularly investment risks.
- The presentation of poorly designed information in an online or mobile format that may incite poor choices, which could result in a "wrong sale" for the consumer.
- Consumers do not understand the full cost of the service, face complicated requirements and inadequate documentation.
- Little or non-existent consumer knowledge and understanding of the complexity of the underlying technologies and systems involved in the provision

7 GFLEC New Insights Report. Millennial mobile payment users: A look into the personal finances and financial behaviours. https://gflec.org/wp-content/uploads/2018/04/GFLEC-Insight-Report-Millennial-Mobile-Payment-Users-Final.pdf?x83489

8 https://www.beuc.eu/publications/beuc-x-2017-073_fintech_a_more_competitive_and_innovative_eu_financial_sector.pdf

of financial products and services, such as the use of algorithms in the provision of robotic counseling.

Suitability of Products and Services Offered

- Inadequate provision of product or service advice due to incomplete or inaccurate customer information (KYC) collection.
- Clients may be treated unfairly due to an inappropriate bonus scheme.
- Companies persuade clients to benefit from particular transactions and services, not because it is in their best interest, but because they offer higher rates or commissions.
- Increased consumer debt due to the ease of access and use of online credit.

Complaints and Claims Management

- The legal definitions of complaint are diverse and diffuse in relation to applications and petitions.
- Consumers do not know that they have the right to complain; or they may know that they have this right, but do not know the proper channels; or they know how and where to file a complaint, but do not receive an adequate response.
- An error in the systems or in the information provided by an automated tool can result in several simultaneous complaints from the affected consumers.
- It is difficult to identify the person responsible for a product or service if different specialized providers are involved in the development of the product or service, or if fintech has partnered with non-financial service providers.
- There may be limitations, biases or errors in the underlying technology that could cause significant harm to the consumer in terms of the claimed value. In addition, the complexity of the technology underlying the claims handling process may be difficult to understand or to challenge by consumers as they seek appropriate remediation of the harm.

Retention of Consumer Records

- As the number of records increases, there may be governance issues, inadequate records and lack of auditing procedures for data.
- Fraud and theft of consumer data if strict security systems are not in place to protect personal and financial data.
- Difficulty to capture and accurately track customer transaction records across social networks and digital platforms.

PRECONDITIONS FOR DIGITAL FINANCIAL CONSUMER PROTECTION

Regulatory and Supervisory Authorities (RSAs) face the challenge of adapting current regulations and supervisory approaches to the increasing use of technological innovations in the provision of financial services, whether by incumbents or fintech. Authorities must find a balance between ensuring the soundness of the financial system, maintaining market integrity and transparency, and ensuring adequate protection of financial consumers (regardless of the channels and providers used to purchase financial products and services), while allowing or even encouraging technological advances.

The supervision of fintech may involve new ways of interacting with these companies or providers, and for this reason we believe it is necessary to raise some prior considerations in order to develop effective strategies and actions for the adequate protection of the consumer of financial products and services.

Ensure a regulatory and supervisory framework for the protection of financial consumers and the timely resolution of complaints

In the survey conducted with the region's ARSs,[9] we identified that the institutional arrangement for financial consumer protection is variable. Some prudential supervisory authorities have powers in this area, others share this responsibility with cross-cutting consumer protection authorities (they monitor the area in other industries), in other cases there is an authority specialized in financial consumer protection, and in other schemes, although the prudential authority does not have a specific mandate in consumer protection, they deploy or coordinate actions in this area.

Therefore, depending on the institutional arrangement of each jurisdiction, the following models are available:

- Twin Peaks: Supervisory and/or regulatory functions in two authorities, one for prudential supervision and the other in charge of supervising business conduct.
- Integrated model: Supervisory and/or regulatory functions in a single authority, with three pillars in-house, one management or equivalent for prudential issues, another management or equivalent for securities market and infrastructure, and one management or equivalent for business conduct and consumer protection.
- Sectoral or institutional model: Supervisory and/or regulatory functions according to the legal activity of the entities, from a prudential and business conduct perspective. That is, one supervisory authority for banking, one for insurance and one for securities

9 In order to deepen the understanding of marketing practices, information disclosure and consumer protection of fintech products in the different ASBA jurisdictions, a survey was circulated with the ultimate objective of developing an overview of the main characteristics and challenges that supervisors may face when confronted with a review of the regulatory body and supervisory intensity for the incorporation of innovative technologies in the financial sector in a responsible, transparent, and competitive manner. The survey was completed by 14 ASBA member jurisdictions, which are: Bolivia, Brazil, Chile, Costa Rica, Ecuador, El Salvador, Guatemala, Guyana, Honduras, Mexico, St. Kitts & Nevis, Spain, Turks & Caicos Islands and Uruguay.

and pensions, and each authority with a directive or its equivalent for consumer protection. In this model the supervision of some industries may or may not be integrated (e.g. banking and insurance, securities and pensions, etc.).

- Three-peaks model: Supervisory and/or regulatory functions in three authorities, one for prudential supervision, one for securities market and investor protection and one independent consumer protection authority with a mandate for supervision, education of financial consumers, and strengthening of financial education among citizens.

It is an essential condition to assess within each institutional arrangement whether the area, board or its equivalent in charge of financial consumer protection tasks has the mandate as well as human and technical resources to supervise financial consumer protection in at least the following aspects:

- Consumer protection risk management;
- Analysis of consumer protection in the pre-contractual, contractual and post-contractual stages of service provision;
- Ensuring adequate provision of information and transparency;
- Anticipation in risk monitoring activities that, like the operational one, are of high incidence in the adequate consumer protection;
- Attention to complaints and claims and their analysis as an input for consumer supervision strategies;
- Capacity to carry out sanctioning processes against supervised entities in the area of consumer protection;
- Promotion for the development of conflict resolution mechanisms;
- Participation in the development of financial education strategies and actions.

The supervisory authorities must have powers to enforce existing laws and regulations (enforcement) for both traditional entities and fintech.

The most common powers available to authorities to enforce the regulatory framework are:

- Voluntary compliance measures: Based on these measures, the authority ensures that the supervised party voluntarily complies with the rules, so that the sanction becomes a mechanism of last resort. They can be binding (generally requests) or non-binding (warnings or recommendations), and these can be the issuance of orders, recommendations, warnings, admonitions or notices.
- Deterrents or instructions: These are provisions or orders that the authorities can impose if they notice situations or practices that potentially or actually affect consumers. They seek the mandatory adoption of measures or the development of action plans aimed at correcting the shortcomings detected.
- Sanctioning measures: Supervisory determinations that, after a procedure (generally administrative sanctioning) lead to the imposition of sanctions and exemplary measures to those supervised for non-compliance with consumer protection regulations. Sanctions may be institutional or personal and include reprimands, financial penalties and even temporary or definitive prohibition of one or more operations or activities. In some jurisdictions the infringement of the consumer protection regime is in itself a cause of punitive aggravation.
- Meta-regulation:[10] With these measures the supervised entities apply risk management mechanisms and the authority supervises the operation of such mechanisms.

10 Cunningham, *Neil. Enforcement and Compliance Strategies*, in The Oxford Handbook of Regulation, Oxford University press, 2010.

To establish cooperation mechanisms between relevant authorities for the active protection of financial consumers.

There are several reasons for supervisors to actively and effectively engage and cooperate with other authorities in charge of supervision in relation to companies providing products and/or services resulting from technological innovations.

One of these reasons is that it helps supervisors to obtain an overview of the implications of fintech (different sectors, cross-border, technology, money laundering, data protection, etc.) and also that it can help to coordinate efforts, avoid regulatory overlaps and identify potential risks. As such, one would expect that there will be a clear cooperation or delegation of roles regarding:

- Consumer protection authority;
- Relevant regulators in each jurisdiction;
- Other financial supervisors in each jurisdiction;
- Anti-money laundering authority;
- Data protection authority;
- Other supervisors outside the jurisdiction;
- Competition authority;
- Telecommunications regulator.

On the other hand, the authorities are expected to show a proactive approach in signing formal cooperation agreements with overseas regulators and supervisors through Memoranda of Understanding (MoU), mainly for information exchange and joint committees to address supervisory issues of fintech. Collaboration on cybersecurity issues and the possibility of supporting centers of innovation are also required within each jurisdiction.

Coordinated regulatory and supervisory approaches and joint analyses help significantly to avoid arbitrage and synchronize the treatment of both incumbents and new fintech service providers with a regional presence.

Ability to adapt licensing and authorization regimes.

In view of the possible expansion of the regulatory and supervisory perimeter of new entities providing digital services and products, the general licensing rules should be able to be adapted to take into account the opportunities, challenges and risks posed by new fintech companies, increasing the focus on the understanding of business models and the nature of new relationships with financial consumers.

The authorities must have these powers in advance so that the expansion of the regulatory perimeter is carried out in a sustainable manner. For example, the introduction of "regulatory sandboxes", in certain jurisdictions with particular characteristics, can play a key role in the licensing processes by providing a mechanism to observe the operations of the new fintech provider before approving its license.

Develop comprehensive financial education strategies related to financial consumer protection, aimed at increasing consumer awareness of the inherent risks of using financial products and services and contributing to the goal of mitigating risks to consumers.

Financial Education (FE) is the foundation of a robust strategy of financial consumer protection, since it allows users to build from their own environment a first line of knowledge and protection that allows them to choose the products and services best suited to their needs and possibilities, to know the attributes, costs and risks of certain products and providers, and especially to know their duties and rights in their management.

We consider it a precondition that the financial supervisor has FE programs or participates in the design and imple-

mentation of strategies and actions. Its experience in the field as a supervisory authority places it in a privileged position to determine the aspects that are fundamental to increasing levels of protection, the aspects on which consumer training should be oriented, as well as the most appropriate ways to build an effective pedagogical approach.

In FE programs, therefore, supervisory authorities should avoid that program objectives be limited to explaining the risks associated with certain technology products or services, but should, to a greater extent, promote preventive attitudes on the consumers of products. It is desirable that programs established in jurisdictions encourage the development and dissemination of specific topics, among them:

- New financial products and services;
- Responsible management of digital tools and resources;
- Adequate identification of incumbents and suppliers;
- Submission and processing of complaints and claims;
- Risks.

In addition, the RSAs may issue warnings and notices to consumers regarding services and providers where significant failures in service delivery have occurred.

To have and/or train teams with digital expertise applied to consumers and technological outsourcing assessment.

Information Technology (IT) supervisors are not usually involved in monitoring financial consumer risks, let alone those associated with fintech. Authorities that have a prudential supervision mandate have groups specialized in IT (operational risk) assessment rather than conduct supervision in general. Therefore, to meet the digital fintech challenge, we recommend that, in order to develop and implement a regulatory and supervisory framework effectively, supervisors should:

- Train and continuously update existing staff to develop and apply sufficient technical knowledge to properly analyze and oversee complex new financial technology;
- Increase the number of IT supervisors available for behavioral monitoring and ensure that they have specific skills relevant to monitoring the products and services offered by fintech;
- Ensure that IT supervisors follow an approach that, based on IT risk, analyses risks to consumers throughout the product lifecycle.

On the other hand, traditional entities and new fintech service providers outsource certain processes or activities relevant to the provision of technology products and services offered online, and these online platform providers may not be located in the jurisdiction where the products and services are marketed.

Although responsibility for outsourced activities should remain with the supervised financial institution, supervisory authorities often review agreements through a prudential approach, i.e. by assessing potential IT risks. In that assessment, they should broaden the scope to analyze most of the contracts signed, or at least a relevant sample, between supervised entities and external technology service providers in relation to products and/or services coming from technological innovations, seeking to establish, among others, situations that may affect the adequate attention and protection of the consumer.

GENERAL CONSIDERATIONS AND RECOMMENDATIONS

In order for fintech to accomplish its ideas and proposals for entrepreneurship, regulators and supervisors are faced with a challenge: to enable suppliers to carry out their business models without undermining consumer protection, creating a fair competitive playing field, the integrity of financial markets and the stability of the financial system as a whole.

The European Banking Authority (EBA) published its fintech roadmap[11] in March 2018, proposing the following actions:

- Address authorization and regulatory perimeter issues related to fintech. This includes the evaluation of the current authorization and licensing processes of fintech entities, and the analysis of regulatory sandboxes and innovation centers.
- Developing consumer protection issues. Issues arising from fintech that affect consumers will be identified, in particular, related to areas where regulation of fintech entities and disclosure of information to consumers is unclear.
- Analyze the impact on the entities' business models, as well as the prudential risks and opportunities arising from the use of fintech. Examine the way in which institutions deal with risks and adapt their internal governance, control and risk management frameworks.
- Promote best monitoring practices for cybersecurity assessment and for the establishment of a common cyberthreat assessment framework.
- Identify and assess Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) risks from fintech entities, technology providers, and fintech solutions.
- Create a Fintech Knowledge Hub that will provide a general forum for integrating the competent authorities.

In this context, many so-called incumbent providers have raised the issue that they would be operating on uneven "playing fields" and regulatory arbitrage risks. In this sense, in order to maintain a balanced "playground" a principle of "same activities, same risks, same rules and same supervision" has been proposed, so that all the companies that carry out activities and have similar risks receive the same treatment in terms of regulation and supervision.

There is currently a debate about the appropriateness of establishing differentiated regulation based on the type, size and complexity of the operations. In this regard, prudential risks should be considered to be assessed considering the combination of the activities undertaken by an institution and its business model, which results in institution-based prudential supervision and the possibility of applying differential requirements.

However, at the behavioral level, specific products and services may carry similar risks for the consumer, regardless of the institution providing them, and should be regulated accordingly.

11 https://eba.europa.eu/-/eba-publishes-its-roadmap-on-fintech

Thus, in order to ensure a fair playground without resorting to regulatory arbitrage, we recommend that the authorities consider the following minimum considerations and recommendations:

The same activities and services share the same risks against the consumer, so the same regulation should apply, regardless of the type of legal entity that supervises them.

To implement this principle, RSAs should devise ways to obtain adequate information from the fintech ecosystem in their jurisdictions in order to monitor technological developments, market segments served, and the ongoing analysis of benefits and potential risks, particularly in terms of consumer and investor protection and financial inclusion.

In this way, we intend to develop and promote the authorities' knowledge of the fintech ecosystem, with particular emphasis on the providers of these products or services, even when they operate outside their natural area of supervision (perimeter). This knowledge can be built, for example, through a centralized public electronic record, containing a list of all fintech companies and their subsidiaries (whether they are within or outside the supervisory perimeter).

The record may be managed by a body other than the supervisory authority, such as a Ministry of Economy or Industry, or a similar entity to chambers of commerce or registrars in charge of managing public records.

The record is only an ecosystem mapping tool which **does not involve any kind of supervision**. It will therefore be necessary to communicate to the public that the fact that a company is registered in the record does not imply any kind of monitoring of these entities. This is why it is highly recommended that the record is not kept by the supervisory authority, as this would avoid generating expectations in consumers and prevent the inappropriate use of the term "record" as a way of giving an apparent status of financial supervision.

We recommend that knowledge of the ecosystem includes at least the following information for all existing fintech (inside or outside the perimeter):

1. Legal or individual company type.
2. Name of the company.
3. Main shareholders of the company.
4. Name of the company.
5. Address, city, country, zip code.
6. Contact details for consumer services.
7. National identification number.
8. Date of incorporation of the company.
9. A pre-defined list typifying the different fintech segments to which the company may belong.
10. A brief description of the products and/or services offered, along with the website and/or mobile application address.
11. The country or countries where the service or product sale will take place, including the location (i.e. country or region) of the collected data.

To ensure a uniform provision of information, financial and competing RSAs should coordinate on the use of a standardized format for collecting the information and allow consumers to easily understand the information contained on the centralized electronic record in a clear and unambiguous manner.

By applying this recommendation to companies belonging to the fintech ecosystem, it will be easier to identify and introduce into the perimeter of financial regulation and supervision only those suppliers that carry out **the same activities that are traditionally authorized by the financial supervisor**, leaving outside the perimeter of the financial supervisor companies whose business model does not require a financial licensing scheme.

Given the constant evolution of the proposed activities in the fintech ecosystem, in accordance with the above

criterion, supervisors must consider whether new forms of business are involved:

- Significant differences with respect to traditional schemes of mass collection of resources from the public or other activities reserved to supervised institutions, for example, in the area of insurance or the stock market;
- Massive models of management or accumulation of money from consumers of different characteristics, even if they do not fit into the traditional criteria of recruitment;
- Activities that generate business models with massive onboarding of consumers that tend to substitute the functionality that traditionally provides a supervised institution, proposing a "disintermediation" or "financial deinstitutionalization". In these cases, each situation must be evaluated in order to consider whether or not it is appropriate to include them in the perimeter.
- Some fintech activities that, due to their size and role, become critical in transactional, operational or management processes in systemic financial institutions or in several financial institutions.

The providers of products and services that are included in the perimeter of financial regulation and supervision must have a licensing guide. Companies that perform activities similar to traditional financial institutions may enter directly under the traditional licensing scheme and the regulation of each jurisdiction, as may be the case of neo-banks and neo-insurers.

However, for those fintech companies that are truly disruptive to their business model and whose application of the traditional licensing scheme is complicated and costly in terms of capital, risk management systems, operations and scope, among others, RSAs may consider working on "licensing with minimum prudential requirements" schemes, so that such companies may carry out their activities conditionally and with certain restrictions within the perimeter of supervision.

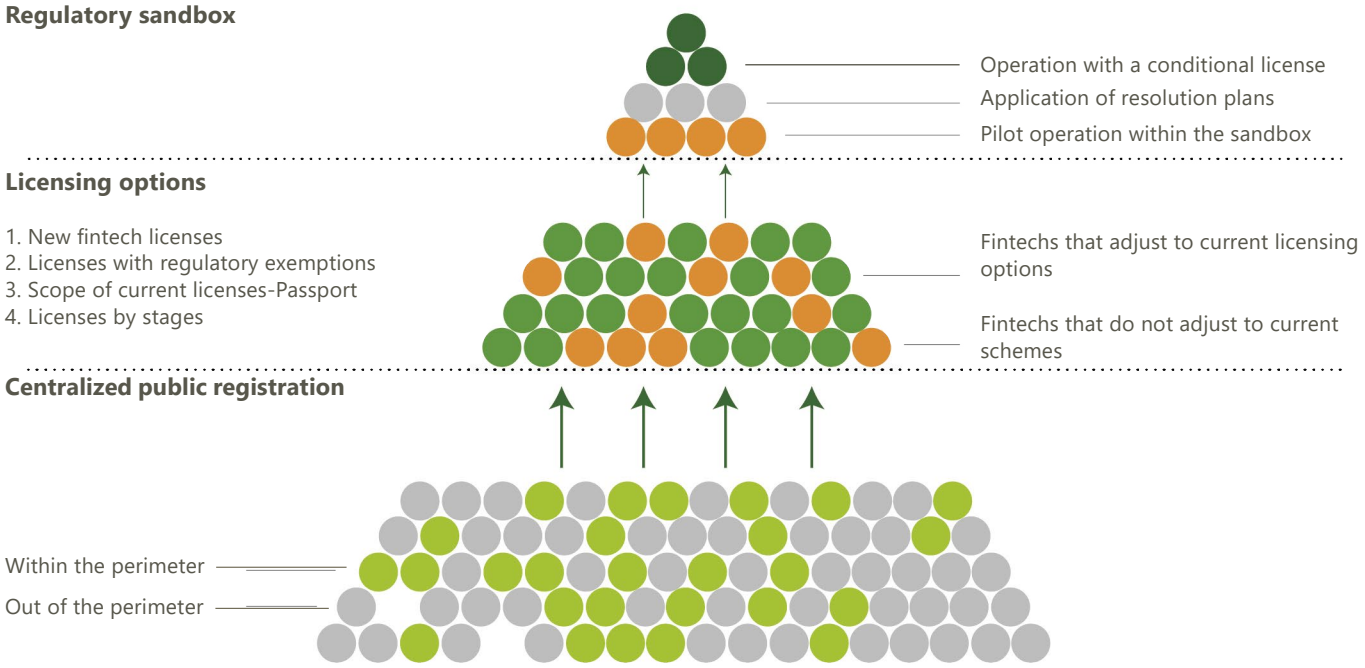
Only for fintech companies with a new, disruptive and sophisticated business model, the RSAs may consider providing controlled experimentation spaces or "regulatory sandboxes", as long as their context and legal framework allow it.

This could allow for temporary permissions from authorities to implement innovative products or services in controlled environments, as well as prudent adjustments to regulations to boost the potential added value to customers, convenience and sustainability over time of these new products or services (figure 1).

When analyzing the disruptive nature of a fintech business model, the authorities should ask the companies for:

- Proof of the novelty of the fintech initiative, explaining in detail its material variation from traditional forms of provision both in the jurisdiction and in more developed markets;
- It should be indicated whether the technology introduces a real novelty in specific processes of the supervised entity: knowledge of the market, segmentation and customer relationship, supervision and risk management, service delivery, attention to complaints and claims, among others.
- The way in which this innovation will affect the business model, especially by strengthening the capacity to establish links with customers and to provide new services;
- The way in which the disruptive scheme or tool will affect the business model, the appetite for risk and the financial and asset condition of the entity.

Figure 1. Registration, Licensing and Sandbox Processes for Fintech



THE SUPERVISORY APPROACH SHOULD BE RISK-BASED BUT CONSIDERING THE PROPORTIONALITY OF SUPERVISORY ACTIONS BY LOOKING AT THE BUSINESS MODEL, SIZE, SYSTEMIC IMPORTANCE, AND COMPLEXITY AND CROSS-BORDER ACTIVITY OF FINTECH.

To maximize supervisory effectiveness and minimize a negative effect on technological innovation by fintech, any supervisory action should, to the extent possible, promote desirable behavior and discourage misconduct by firms, while limiting compliance costs.

If a proportionate approach to supervisory action is not taken, innovators will fear being punished for every mistake and will be less assertive in trying to develop the next application of financial technology, so that more time and effort will be devoted to compliance. For example, penalizing a company for a small technical infringement of information security or consumer protection regulations that causes little or no harm to consumers is likely to push the company to spend more resources on lawyers rather than improving its service offering.

In the event that a misconduct on the part of fintech service providers is identified, we recommend that supervisory actions be based on two criteria: 1) whether the company acted intentionally or negligently, and 2) whether the company's action resulted in actual harm to the consumer. In this way, supervisors, using criteria of proportionality, will determine the sanctions, where unintentional and harmless actions that do not generate adverse material effects may not receive any penalty, and intentional, negligent and harmful actions with the consumer receive a severe penalty.

From this perspective, the possibility of blocking innovation processes will be diminished, but at the same time there will be clear signals for suppliers concerning misconduct that fails to protect consumers.

It is important to emphasize that the application of this recommendation should consider the possibilities that the legal frameworks offer to supervisors, so that it should always be left to the discretion of the authority to estimate their origin, as well as to define minimum applicable standards and procedures to verify their compliance.

Adopt technological neutrality in regulation so as not to inhibit the use of certain technologies or generate biases in favor of others.

Fintech's business models are not uniform, so regulators must adopt technology-neutral rules that neither favor nor disfavor any particular fintech application, to create a balanced playground for innovation.

When there are differences in technologies, supervisors must be careful to recognize the different risks in particular fintech tools and applications.

Promote harmonization and remove regulatory duplication that could affect the protection of financial consumers.

In the region, some financial RSAs do not have full (or partial) powers in consumer protection issues such as customer service, marketing, advertising, information and advice, contractual issues, complaints and claims. Similarly, some authorities are identified as regulating the issue generally by applying the regulations to fintech companies not specifically but by virtue of generic competence, so that in certain cases a patchwork of regulations governing financial technology companies may be present and may create duplicate requirements from multiple regulators, e.g., in the consumer disclosure requirements that are often the centerpiece of consumer financial protection regulations.

Therefore, financial regulators and supervisors need to work closely with consumer protection authorities in designing an action plan for updating consumer protection regulation that pays particular attention to the needs of financial consumers and retail investors and the risks to which they may be vulnerable.

In the regulatory component, it is essential that, in the institutional arrangement, the preparation of the regulations applicable to fintech companies and activities be undertaken by an expert authority (either the supervisor or another authority with the collaboration or active participation of the financial supervisor). This authority should have the power to monitor the development of the fintech industry, be aware of regulatory developments and best practices in this area and prepare regulatory initiatives that incorporate specific consumer protection aspects.

In addition, the authority must constantly assess the relevance of the regulatory perimeter to determine when an activity outside of it needs to be subject to financial regulation and supervision, due to the conduct of a financial activity or the acquisition of massive amounts of customers' money.

When having a regulatory overlap, regulators should strive to coordinate and centralize these activities to streamline the process and reduce the regulatory burden on financial technology firms, or seek new powers or attributions to address the growing expansion of financial technology in services such as collective financing, payment platforms, peer-to-peer lending, and virtual banking.

Depending on the context of each jurisdiction, the effectiveness of inter-agency coordination should be assessed. If the regulatory framework in which the authorities operate allows it, specific assignments or delegations of activities could be considered to define responsible authorities, avoiding that, in view of the risk of overlapping competences, what might occur is the absence of effective supervision.

Financial supervisors should encourage coordination between overlapped supervisors, as appropriate, to make the supervision of fintech more effective.

Fintech companies collect large amounts of data from their clients, including confidential personal information (biometrics) and financial records. They also increasingly collect alternative data, such as that related to a client's

online spending behavior and social networking patterns to track a customer's fingerprint. This collection of personal information used for financial products and services leads to different supervisors having supervisory objectives over the same company, in this example, a financial supervisory authority and a personal data protection authority.

Thus, current regional regulations on personal data protection, derived in most cases from the European Data Protection Regulation (GDPR), already cover some of fintech's data protection concerns. But developments in technology are continually expanding new areas in which additional or refined regulation may be required, therefore, the coordination between supervisory authorities as well.

Supervisors must monitor fintech activity outside the regulatory perimeter, keeping an eye on financial technology trends and considering their potential impact on consumer protection.

Supervisory authorities are a key part of the overall consumer protection framework, and given the pace and scale of technological innovation, it is increasingly difficult for regulators to determine what is regulated and what is outside the perimeter. For this reason, when innovation relates to services and products that are out of reach, it is necessary to be aware of the risks that they may pose to consumers and have a rule to involve them within the perimeter.

A suggested rule may relate to the scaling-up of the number of clients by a fintech outside the perimeter. When this number reaches a percentage above the average number of clients of other monitored fintech it should be brought within the perimeter of supervision, and this rule should be clear, coordinated with other authorities and communicated to the market.

In addition to the above, the criteria set out in page 20 may be considered.

GUIDELINES AND RECOMMENDATIONS CONCERNING THE DUTIES AND RIGHTS OF DIGITAL FINANCIAL CONSUMERS

In addition to the considerations and recommendations set out in the previous section, and the national consumer protection frameworks that apply to all financial providers, whether they are traditional or fintech,[12] financial innovation companies have duties of protection towards their consumers, which **are transversal to** the identified segments of products (deposits and credits, payments, insurance, investment management, infrastructure and support of markets and capital accumulation). On the other hand, consumers have rights but also duties in this new environment.

Fintech's responsibilities towards the consumer

In order to deliver the right products to their customers, fintech puts the consumer at the center of everything they do. However, to maintain this idea of value that distinguishes these companies, the traditional risks faced by consumers must be considered: financial, fraud, misuse of personal and financial data, profiling, cyber-crime, among others.

Also, new risk approaches related to the type of behavior that companies and the market can generate in consumers must be considered, as well as the possible relaxation of verification controls due to the personalization of products and the digitalization of processes.

The following is a set of minimum considerations and recommendations that authorities and fintech service providers should take on account when addressing consumer behavior issues.

Perform consumer protection risk assessment throughout the product life cycle: product development, sales or transactional process, and post-sales.

Consumer protection risk is based on the definition of misconduct risk as the risk that the behavior of a financial services entity, throughout the product life cycle, will cause undesired effects and impacts on customers. There should be transparent and effective mechanisms for information disclosure and advice to consumers.

Fintech associations have almost uniformly raised the concern that they are required to provide too much information, resulting in consumers not reviewing all the information presented to them, and this may be exacerbated in a digital environment. This appears to be supported by analyses conducted by the European Insurance and Occupational Pensions Authority (EIOPA),[13] which highlights that consumers may be less inclined to read standard disclosure documents describing product details when shopping online.

12 https://www.ftc.gov/policy/international/competition-consumer-protection-authorities-worldwide

13 https://eiopa.europa.eu/publications/opinions/opinion_on_sale_%20via_the_internetpublished.pdf

The European Commission states in its Action Plan that the feedback received from the industry suggests that current pre-contractual disclosure requirements are not suited to the digital world. Industry responses to the EBA on the *European Commission's Green Paper* on Retail Financial Services[14] suggested the use of more interactive and attractive platforms, which are suitable for smartphones or tablets and which improve consumers' understanding of financial products.

Customer adoption of new digital services requires that access to these technologies be explained in comprehensible language, that the technologies be popularized and validated by a competent body (e.g., that an electronic transaction meets the standards of a certification body), and that the terms and conditions under which the technology is provided be clearly worded, so as to give the customer confidence in its adoption.

The provision of information to consumers is therefore key in established consumer protection frameworks and tends to develop through the different stages of the contractual relationship between client and supplier. Some recommendations for innovative disclosures that can be promoted are:

i) During the contract's term

- Suggest to new companies and incumbents offering fintech products to adopt the four behavioral design steps in their products and services:[15]
    a) Capture attention: Align the product and service with the consumer's need; incorporate intelligent reminders and alerts; interrupt habits and redirect attention; make human contact available.
    b) Inspire confidence: Make the process transparent; use visual signals and safety signs; watch the tone and style of communication with consumers.
    c) Simplify the decision: Facilitate understanding of selection; structure the choice in a way that helps consumers to decide.
    d) Facilitate action: Eliminate requirements that may involve multiple steps or uncertain steps; give the consumer an idea of the progress he or she is making, from claiming to have already taken the first step to reminding him or her that the process is nearing completion.
- Make use of infographics and interactive tools to present difficult information; or make use of videos to explain complex information to consumers; create guides that fit the medium; make use of virtual quotes, and allow customers to open demos to try out new products and services. All of the above is aimed at helping consumers make a decision regarding the acquisition of a financial product or service by being clear about: the type of operation to be executed, the scope of the service to be received, the management of the resources granted, the inherent risks and associated costs.
- Since the information related to product terms and conditions is intended to be read by a consumer in an easy way on a smartphone or mobile device, the use of text may not be practical, so it is more beneficial to consumers if companies choose to present the information and warnings in the ways outlined above, but companies should be required to oblige customers to spend time on the terms and conditions screens and decrease the possibility of them ignoring this information.
- The full ordinary costs of the product, expressed both as a sum of money and as an annual percentage rate, should be disclosed, as should the costs of any other product or service included in the same package as the main product. The dates on which payments are to be made and the corresponding amounts, as well as the late payment fees and the time at which they apply, should also be clearly presented.

14 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:52015DC0630&from=EN

15 Katy Davis, Maddie Kau, and Abigail Kim. Behavioral Design for Digital Financial Services.

- The customer should be informed simply and transparently about the use and handling of consumer data, and effective ways of reporting such use and data handling practices should be developed before the product or service in question originates, in accordance with personal data protection rules.
- The nature of automated investment management limits human intervention, but access can and should be provided to a human operator to assist the customer throughout the process, if required. This is particularly relevant when the client's financial or digital knowledge is low.
- There must be a balance between opening the products and services and closing them. In most digital products and services, the promotion and opening of products is done at a distance, without personal interaction during the application for products and in short procedures. However, when products and services are closed or canceled, some kind of friction gets in the way and limits the right of financial consumers to terminate contracts.

ii) During the execution of the contract

- Fintech companies must not engage in conducts that lead to contractual abuse or agree to terms that may affect the balance of the contract or convey to an abuse of a dominant contractual position.
- Overtly unfair terms or conditions should be avoided, such as those related to the possibility of the termination of the service at any time by the provider; assigning obligations to the consumer but not to the provider; exonerating the provider from any liability, in particular for operational failures and service availability; lack of product statements; and contractual terms in a language other than that of the jurisdiction.
- Comply with the conditions announced on websites, social networks, physical media, mobile applications and in the push strategies not requested by the customer, compared to the real functionalities of the product or service provided.
- Refrain from using false or unverifiable figures and testimonials and improper description of the characteristics of digital financial products.
- Procedures should be in place to inform consumers of any cyber incidents that have occurred and where the confidentiality or integrity of personal and/or financial information could be affected, as well as the measures taken to remedy the situation.
- The sharing of information should be clearly distinguished from the provision of advice to avoid uncertainty among clients. In particular, fintech service providers must distinguish between consumer-oriented and advice-oriented tools. That is, they should clarify when a recommendation/general information becomes an advice; distinguish between partially automated processes and other automated tools; and establish equal monitoring requirements for both automated advice and recommendations provided by a human advisor.

iii) During the termination of the contract

- Only if the nature of the product allows it, the provider must facilitate the customer's right to withdraw from a contract and rescind it, notifying him or her of the withdrawal within the period stated to that end, without having to justify the decision and without any penalty. In those cases, the appropriate charges will be made according to the type of service and the degree of execution of the operation.
- The procedure for the termination of the contractual relationship must be clearly established, so that it can be performed through the channels made available for the conclusion of the contract, and without imposing greater requirements on customers than those requested at the time of conclusion of the contract to terminate the service.

Incorporate suitability requirements.

There is a risk that customers looking for a specific product or service will respond in a biased manner to questions from suppliers looking for the most suitable option for them. In general, it has been observed that consumers resort to this action to a greater extent when they inter-

act online or on their mobile phone, compared to when they are in front of the provider or financial intermediary.

Therefore, fintech's suppliers must adopt suitability requirements towards their customers to ensure that any product sold is appropriate to the consumer's needs and circumstances. The key suitability provisions are associated with:

- Know Your Customer (KYC) process in which fintech collect sufficient and verifiable information to better segment its current and potential customer base and evaluate whether the product or service is suitable for a particular consumer before offering it. For example, in the case of personal loans, segmentation should pay attention to actual repayment capacity and direct efforts to cases that show adequate use of funds.
- The human and technical resources of the fintech industry must be oriented towards ensuring that the recommendation given to a client or potential client is the most appropriate for his or her needs, expectations and possibilities.

To have an adequate complaint management process.

An efficient complaint management system is considered an effective indicator of procedures, controls, training needs and service levels in all companies. Examples of adequate complaint management include:

- Centralization of all complaints within the companies with clear processes within all the departments involved.
- Implementation of specialized software solutions for complaint management.
- Customer communication strategies, including social networks and popular digital channels.
- Proactive follow-up of complaints through automatic notifications.

However, in different jurisdictions there are often regulations that scatter complaint management and in some cases are not always consistent, making it difficult to design effective procedures. For example, there are varying definitions of what a complaint, claim and request is.

When dealing with complaints, fintech must:

- Treat equally the entry of any consumer complaint, request or inquiry regarding the product or service provided that cannot be resolved within 24 hours. This should be entered into the management system and include identification of the main cause of the problems, with the purpose of ensuring that similar complaints are resolved as a whole rather than focusing solely on the individual complaint.
- Complaint resolution times, mandated in the regulations, must be complied with and the consumer must be informed when a complaint will require more time for resolution indicating the reason and the final response date.
- Companies should monitor expressions of dissatisfaction in digital media and platforms where they have a presence, and when the expression of dissatisfaction is identified the consumer should be invited to make a specific formal statement and initiate a complaint through a formal process.
- There must be a database with the complaint register (log) detailing each complaint, date received, department in charge of the solution, actions taken to resolve, date of resolution, etc. The maintenance of this database must be protected in a durable medium and kept for the time indicated by the regulations to demonstrate compliance with the regulation and to be used to identify the main cause.
- Consumers may have different preferences about how they would like to make and manage their complaints. While one part of the population prefers to engage in direct communication with the company, another part, particularly those belonging to a younger generation, prefers and expects being able to make complaints through digital channels.

In general, entities should be able to offer both options to consumers: digital and physical. Fintech's investment management service providers should offer physical contact if the complaint or dispute could not be resolved digitally, or when the client explicitly requests it.

Treat clients fairly when handling complaints.

In the complaint and claim handling component, the regulatory framework should clearly establish the obligation of incumbents and new service providers to deal with consumer complaints and claims in a timely and effective manner. It must also provide for the procedures to be followed by the RSAs or other qualified consumer protection authorities, within their respective areas of competence, in dealing with complaints made by consumers. Such complaints should constantly feed the supervisory process.

From a consumer protection perspective, the underlying principle with respect to complaint handling is that any innovative methods used by fintech suppliers to address such complaints should treat consumers fairly.

The same methodologies that are used in pricing and underwriting should not be used to "optimize" settlement proposals on the statistical probability that the insured/claimant will accept the offer, rather than using the fair value of the claim.

Current existing processes, particularly in the insurance industry, are heavy on human resources, with onerous administrative tasks and some decision steps are left to discretion. This has created room for Fintech to innovate in the use of machine learning and pattern recognition to achieve efficiency gains, time and cost savings, as well as accuracy and consistency in claims analysis by scanning manuscripts and unstructured documents that expedite and detect false claims. Therefore, incumbents and fintech companies must:

- Ensure that consumers receive high quality advice especially regarding complex products that may be difficult for an average consumer to understand, so the client should be helped in the claim process.
- The written procedure and other communication mechanisms, as mentioned in section 2.1, must be available to the customer for the effective and proper handling of complaints.
- Accurate information regarding the timeframes for informing the consumer of the outcome of the complaint, the time for consideration of the settlement offer, and the time for resolution of the complaint after acceptance of the offer by the consumer should be provided.

In complaint management, suppliers are doing advanced analysis (analytics) and machine learning with personal data to create early warning systems and collect practical information that will prevent accidents, and also simplify and speed up the processing of complaints. Examples include using artificial intelligence to detect and verify recurring accident points, estimate repair costs, and identifying potential fraud.

Therefore, fintech companies must:

- Take measures to protect consumers' personal data during collection, processing, correction and exchange, and ensure the security of information and data, adhering to privacy and information security standards designed to protect these assets from cyber incidents, breaches or unintended use.

Safeguard the storage of consumer records.

As the number of customers' digital transactions increases, so does the risk of loss of consumer records: conditions, instructions, decisions, and any other details that demonstrate that the company acted in the best interests of the customer and in compliance with its duties. It has been

noted that fintech's digital investment advisory services have sometimes been unable to review the individual financial advice provided to some of their clients because they have not been able to access client records to determine whether they were affected by a financial loss.

Also, in outsourcing digital record keeping to third party providers and in particular to providers with cloud infrastructure, the event of data corruption or being subject to cyber-attacks has been identified as a risk.

In view of the previous situations, some financial regulators have mandated digital record-keeping by companies to ensure consumer protection in financial services. In the United States, SEC 17a-4[16] and MiFID II[17] in Europe require 100% capture and retention of all digital interactions and immediate access to them for up to seven years.

Therefore, digital service providers that supply digital financial advice should:

- Have strong maintenance systems over the advisory algorithms and the records that are generated. Ideally, the systems implemented should effectively control, monitor, review and record changes made to the algorithms. In the same way, digital advice providers must be able to justify the reasons for updating the algorithm that supports the advice given to the consumer and be able to generate automated reports that can be downloaded and provided to the supervisor when required.
- Any fintech company is expected to describe how it manages customer transaction recording, transaction processing, and internal controls that will enable the company to protect consumer data and ensure the efficiency of its processing. Accordingly, the company should address in its business plan: (i) information technology program; (ii) compliance management program; (iii) plan to provide independent testing of systems and controls; and (iv) third party risk management system.

Fintech's Consumer Rights and Responsibilities

In general, customers and users of financial services (fintech or traditional) are protected by rights and responsibilities under financial consumer protection regulations. However, there are rights and responsibilities that are specific to the digital environment and that increase consumer confidence in the effective functioning of digital financial products and services.

Rights

- Receive publicity and information that is objective, timely, complete, impartial, clear and verifiable on the characteristics of the products and services received.
- Receive information that allows and facilitates comparison and understanding of the different products and services being offered.
- Receive products and services with safety and quality standards, in accordance with the offered conditions.
- To know in advance the rates (costs) of the products and services offered.
- Respectfully submit queries, requests, applications, complaints or claims to the company and the supervisory authorities.
- In the case of investment clients, that orders are executed in accordance with the instructions given.
- In the case of an investment client, they must receive individualized recommendations with relevant elements of the type of operation that will allow them to make decisions based on the information provided by duly certified professionals.

Responsibilities

- To provide the company in a complete and truthful manner with the necessary information for its involvement, as well as the information required to give investment orders.

16 https://www.finra.org/sites/default/files/SEA.Rule_.17a-4.Interpretations_0_0.pdf
17 http://www.cnmv.es/portal/MiFIDII_MiFIR/MapaMiFID.aspx

- To attend the interviews and/or visits that are required within the policy of knowledge of the client.
- To provide the necessary information for prevention and control of money laundering and financing of terrorism, before signing any contractual relationship.
- To sign contracts for the provision of services, after reading and understanding them.
- Meticulously manage the tools and access channels (insurance) provided by the supplier.
- Authorize the inclusion of the data and report of the credit and stock market sharing to information centers or databases.
- Timely payment of fees or commissions resulting from the services provided, in accordance with the established rates.
- To establish the guarantees to which it is obliged in accordance with the laws applicable to the product or service.
- In the case of an investor client (not an expert), provide the information required to establish his or her risk profile.
- In the case of an investor client, order the operations intended to be executed by the means established by the company in a clear, orderly, and precise manner.

SPECIFIC CONSIDERATIONS FOR MAJOR FINTECH PRODUCTS IN THE AMERICAS

In order to deepen the understanding of marketing, information disclosure and consumer protection practices for fintech products in the different ASBA jurisdictions, a survey was circulated. The ultimate goal of this exercise was to develop an overview of the key features and challenges that supervisors may face in reviewing the regulatory body and current supervisory practices, in order to identify how to best incorporate innovative technologies into the financial sector in an accountable, transparent, and competitive manner.

For each fintech product or service identified as having the greatest use and/or potential for use in the financial sector in the Americas, the main focuses are determined in terms of marketing, disclosure, and user protection practices.

NAME	DESCRIPTION	SEGMENT	SPOTLIGHT
P2P Loans-Consumers-P2B Loans-Business-P2P Insurance	(i) Online platforms where people borrow from funds provided by other people or institutions, including financial institutions-Platforms where people and institutions provide online loans to businesses, (ii) Platforms that connect investors with insurance claimants.	Deposits and credits-Insurance	• Provide clear guidance on investment risk. • Provide clear costs, fees and commissions for the borrower. • Inform how and when the investor will be paid back.
Consumer loans based on non-financial data.	Companies that use non-financial information to grant loans. Targeted to the excluded. They also offer the service to financial institutions.	Deposits and credits	• Possibility of being financially excluded. Methodology and criteria used for the segmentation and granting of credits.

NAME	DESCRIPTION	SEGMENT	SPOTLIGHT
Virtual banking	Newly created financial institutions (with their own banking license or using a third party's) with multiple financial products and whose distribution is exclusively digital.	Deposits and credits	• Offering human attention, especially in the opening and closing processes of products. • Long-term asset support.
Integration between the cell phone operator and the financial institution.	Integration of several financial services within the product portfolio of a cellular operator through the acquisition of a specific license.	Deposits and credits	• Distinguishing between the telephone company operations and the financial operations for the handling of products. • Transparency in the costs of products. • Preventing the undesired opening of a financial product due to possessing a telecommunication service.
Automated savings in social networks from user accounts to a P2P intermediary.	The user authorizes an application (bot) in his or her social media messaging system to check his or her (current) bank accounts. The firm managing the bot instructs another firm to transfer the estimated surplus as an investment in a P2P intermediary or to a financial institution's digital wallet.	Deposits and credits	• Disclose how the money is disposed. • Be clear about the transfer limits, periodicity, suspension of service and attention channels.
Supermarket: comparison of financial products	Online platforms that compare different financial products and their characteristics, without providing advice. Income from referrals.	Market infrastructure and support	• Provide information on the independence of the service provider, who the sponsors are and any interest conflicts. • Disclose all of the service management charges.

NAME	DESCRIPTION	SEGMENT	SPOTLIGHT
Integration of social networks-payments-finance-commerce	Consolidation of online and physical store, social network, messaging, payment instrument, banking, investment and other financial operations in a single business cluster.	Payments	• Handling cyber security issues. • Protection of personal data. • Transparency in costs and fees. • Transparency of the financial service provided.
API credit card payments.	A platform that offers businesses and companies to integrate credit card payments into their systems in a way that is transparent to the purchaser.	Payments	• Handling cyber security issues. • Protection of personal data.
Payment portal-intermediary	Solutions for businesses to accept, authorize and process payments via multiple channels, different currencies and countries and different financial institutions. They are also an essential service provider for other fintech products.	Payments	• Handling cyber security issues. • Transparency in costs and management of business resources • Trade resources transfer periods. • Personal data protection.
Open Banking	Opening of APIs (application program interface) to third parties, i.e. connectors that allow third party companies to easily integrate their developments with the bank's financial data. The consumer will have several app stores of financial services that will offer insurance services, traditional credits or deposits along with innovative peer-to-peer (P2P) payments, crypto-currency	Payments	• Be clear about which companies are considered legal. • Provide clarity and control over what is to be shared. • Making sure that consent is transparent and traceable. • Make trade-offs easy and consistent. • Provide consistency and clarity in consent and access to control panels. • Enable individuals to withdraw consent and re-authenticate themselves accordingly.

NAME	DESCRIPTION	SEGMENT	SPOTLIGHT
	exchange, international currency exchange, mass financing and cross-border shipping.		• Guarantee secure payment protection. • Provide people with access to their balances before they make a payment. • Establish the obligation to protect their customers.
P2P/B2B foreign exchange transactions	Solutions for buying and/or selling foreign currencies for individuals and companies, with bilateral exchange rate settings.	Payments	• Complete the process of getting to know the client. • Perform regular reporting to the LAFT authority. • Provide clarity on costs, commissions and exchange rates.
Distribution of sophisticated financial products directly to retail users.	Use of digital channels such as social networks, online games and similar to offer sophisticated financial products such as leveraged derivatives (contracts for differences and similar) to people without financial knowledge, emulating gambling or games.	Investment management	• Risk disclosure for investment in sophisticated products. • Offering human and specialized contact in response to requests and claims by investors.
Automated advisors (pensions or investments)	Automated solutions for asset management through customer profile analysis. Connects with brokerage houses for asset management.	Investment management	• Explain the algorithm's assessment. • Provide clear client profiling. • Disclosure of investment risk.
Smart contracts	Technological protocol that facilitates, safeguards and executes contracts/agreements. Even in early stages, there are several projects underway in global financial institutions.	Market infrastructure and support	• Inform that the product is automated. • Explain beforehand what the contract is about and under which assumptions.

NAME	DESCRIPTION	SEGMENT	SPOTLIGHT
Use of social network data for financial purposes.	Collection and analysis of data obtained from social networks to be used by financial institutions in the evaluation of clients.	Market infrastructure and support	• Financial exclusion potential. • Transparency in the authorization granted to access personal and financial data as well as profiling. • Handling cyber security issues. • Protection of personal data.
Analysis of customer behavior data	Platform that provides financial institutions with updated information on customer behavior in a variety of environments: social networks, mobile phones, others.	Market infrastructure and support	• Disclosure of the information source. • Explicit authorization by the clients.
Automated interaction with financial users	Speech recognition and speech synthesis system, combined with artificial intelligence to act as the first point of contact for customers calling for assistance or seeking to perform operations.	Market infrastructure and support	• Compliance with data protection standards when using biometric information. • Existance of second instance (human) support mechanism in case the primary support process fails.
Collective micro-financing	Platforms that allow micro investments in new or small companies that require moderate amounts of capital. The investor becomes a shareholder in the company. It includes the different modalities of collective micro-financing, which include or may include financial elements to be analyzed such as: (i) Real estate, and (ii) Capital	Capital raising	• Provide information on the risk being taken. • Clear information on assets, profitability, access to resources and availability. • Transparency in resource management.

NAME	DESCRIPTION	SEGMENT	SPOTLIGHT
Parametric insurance based on blockchain.	Documented insurance contracts in a blockchain and with incident payments executed by an intelligent contract tied to an independent information source.	Insurance	• Transparency during the execution of the contract. • Provide information on the risk being taken.
Products and services involving cryptoactives	Integration of payments with cryptoactives-Cryptobased interbank foreign exchange trading platform-Foreign exchange transactions using cryptoactives-Cryptoactives electronic wallet-Electronic wallet of legal tender and cryptoactives-Online trading platforms for cryptoactives-Funds in cryptoactives-Registration of property through cryptoactives.	Miscellaneous	• Risk disclosure to the investor. • Limitation of its use as a legal tender. • Risk of money laundering and financing of terrorism. • Risk of cryptoactive agents present in a digital or physical wallet being hacked. • Handling cyber security issues.

ALTERNATIVES FOR A CONSUMER PROTECTION AND MISCONDUCT SUPERVISION MODEL IN THE NEW TECHNOLOGICAL ENVIRONMENT

Financial products and services can be complex in the fintech environment and financial decisions involve uncertainty, furthermore, they require consumers to make a risk assessment for which they have no experience. The consequences of their decisions can be significant. Therefore, consumers need assistance and protection, and must trust technology-based financial service providers when making these decisions.

Although providers should design and market products and services in the best interests of their clients, there may be situations which encourage inappropriate behavior by providers towards users, even unintentionally. This has an impact on both the reputation of the financial sector and on stability. Thus, adequate supervision of misconduct risk and a sound consumer protection scheme are necessary to avoid these risks.

Supervisory practices can be framed in two alternatives. The first is the adoption of a risk-based supervisory model for financial consumer protection; the second is the implementation of a proven accountability program for financial consumer protection.

Risk-Based Supervision Model

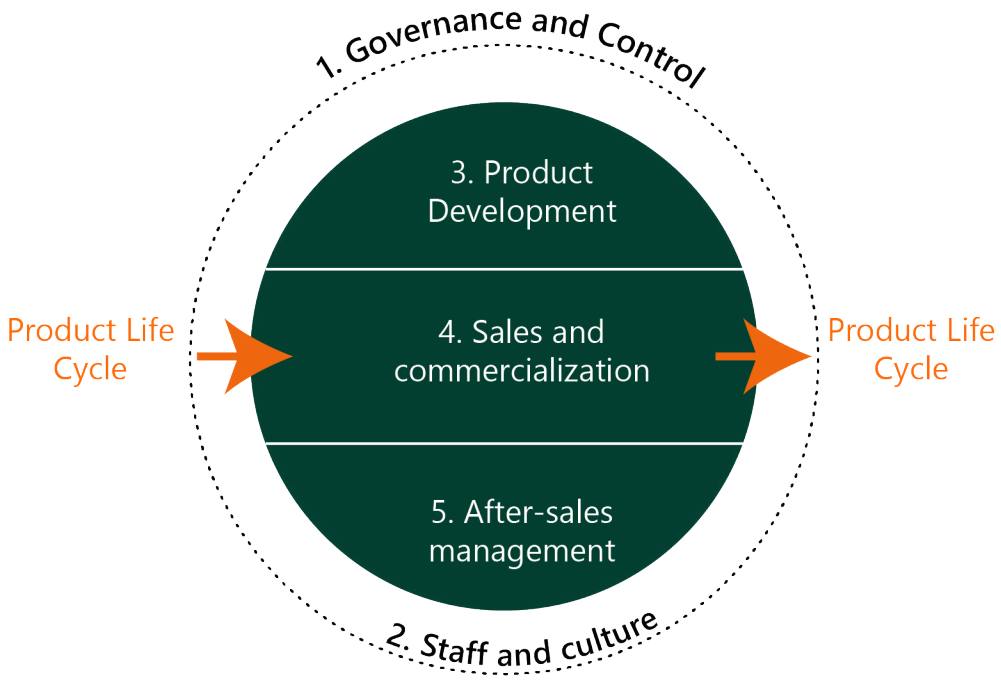
The first alternative focuses on the definition of misconduct risk as the faulty behavior of a financial service entity that may cause undesirable impacts for consumers. Supervisors who have assessed this risk have done so by examining the nature and scope of the institution's products and how the institution manages the risks that its products and other commitments affect its consumers.

Leading financial conduct authorities in Europe, Oceania, and some of the Americas have broadened their scope to assess misconduct risk, recognizing that risks to consumers can stem from the company's strategy, business model, governance, corporate culture, and business partners, as well as other internal structures of the entity foreseen in the construction of the product throughout its life cycle.

The consumer protection risk supervision model can be applied to fintech and incumbent product and service providers that are within the perimeter of supervision under any licensing scheme, whether traditional, minimum prudential requirements (or limited) licensing, or regulatory sandbox. Figure 2 illustrates this model and its elements.

The supervision model has characteristics that are intrusive in nature. It evaluates the design of a control protocol and then seeks concrete evidence of how effective the control is; reviews the policies and procedures used in the construction of the product or service; observes the decisions of the board of directors and key committee meetings in the design and implementation of the product; performs a walk-through into the systems and processes by performing substantial tests on the consistency of the application of the controls, and; interviews a selection of personnel from different levels: board, compliance, risk functions, human resources, product development, marketing and sales personnel.

Figure 2. Risk-Based Supervision Model



i) Governance and Control
Decisions that affect customers occur at all levels of the company. However, in assessing the company's decision structures, the goal is to determine the extent to which a company has implemented effective governance and control and the measures that allow for the identification, measurement, management and effective mitigation of the risk of inadequate consumer protection.

The evaluated issues should be:

- Fintech products and services supplier considers the risk of inadequate consumer protection when developing its strategy or risk appetite;
- Business and control functions provide risk identification, measurement, monitoring and management;
- People responsible for risk identification, assessment, mitigation and monitoring are clearly defined.

ii) Staff and Culture
The supervisor must evaluate whether the staff of the fintech product and service provider has an effective consumer-focused culture. This is done by reviewing whether:

- The company's board of directors and management establish and instill a customer-centric culture through their commitment to treating consumers fairly;
- The company designs and tests services and products specifically with the interests of consumers in mind;
- The company has a clear communication with customers;
- The products and services provider engages constructively with consumers when they submit applications and handles complaints, claims and appeals fairly; and
- Staff members are encouraged to sell appropriate and transparent products to the consumers for whom they were designed.

iii) Product Development.
Among other aspects, we reviewed:

- The degree to which the firm in the design stage reviews all services and products to reasonably meet the needs and expectations of customers; and

- Assesses whether the marketing and distribution areas create adequate safeguards to protect their customers.

iv) Sales and Transactional Process Stage
Attention is paid to:

- The degree to which a company ensures that a consumer understands the products being offered and that they meet their needs;
- Whether products are sold in the right way to the right people;
- Whether commission incentives are adjusted to the transparent sale of products;
- Whether digital distribution channels are safe and clear to consumers; and
- Whether the contracts of fintech product and service providers or incumbents with third parties comply with personal and financial data protection regulations. If this is not the case, amendments to these contracts will be required.

v) After-Sales Management Stage
Items to be assessed:

- The degree to which the company designs and reviews after-sales processes to meet customer needs and expectations;
- The processes designed to deal with complaints and claims, and the number of cases solved in favor of the company and the client; and
- Whether the systems and controls favor expedited customer service and do not create unreasonable barriers in the after-sales process.

Demonstrated Accountability Model

The second alternative of supervision proposes to implement a Demonstrated Accountability program as **long as the regulation allows the supervisor to exercise his mandate through a non-intrusive supervision model.** This alternative is possible in scenarios where multiple providers are outside the perimeter and carry out activities that are not subject to the financial supervisory regime but to other supervisory and control authorities; or in situations where there are **numerous subjects bound** by a regulation and **supervisory resources are limited**.

According to a combination of different sources, the concept of "accountability" can be defined as the obligation or willingness of an individual or an organization to be accountable for its activities, to accept responsibility for them, and to make the results visible in a transparent manner.

In this context, Demonstrated Accountability would only cover those fintech products and services that are outside the scope of supervision but which, by their very nature, are engaged in activities that the authorities consider to be close to traditional ones. In scenarios where a large number of service providers are continuously appearing, the use of the Centralized Public Electronic Registry (described in section 3) would be of great help in determining who is carrying out such activities, and thus be able to monitor the relevance of reviewing the rules of the perimeter.

The demonstrated accountability model contains three elements: accountability, control and evidence. Each of these are necessary to achieve a standard of proven accountability. Consequently, failure in one of these elements would result in the inability of the organization to achieve that standard and prove it.

The first element is **voluntary accountability**, which is achieved through the implementation of an effective financial consumer protection and conduct risk management program by a fintech company. This involves the policies, procedures, activities and other initiatives implemented on a regular basis in the company, which impact risk management or relate to compliance with regulations on financial consumer protection.

Evaluation of the voluntary accountability program involves the following stages of risk management:

Stage 1 determines the extent to which an entity has implemented effective control and governance measures that enable the effective identification, measurement, control and supervision of consumer protection risk.

Stage 2 assesses whether the entity has an effective consumer-focused culture where there is commitment and appropriation to consumer protection from senior management and across all areas; whether entities design and test products with consumers' interests in mind; and whether they communicate clearly with consumers to help them make informed decisions: if they engage constructively with consumers who have questions or complaints and treat claims fairly, and if they encourage their officials to sell appropriate products to the consumers for whom they were designed, mistakes are corrected fairly and conveniently.

Stage 3 assesses the extent to which the supplier designs and reviews all consumer products to meet the reasonable needs and expectations of customers. For example, whether marketing, advertising and distribution arrangements are adequate, and safeguards are placed correctly to protect consumers.

Stage 4 assesses the degree to which the company ensures that the consumer understands the products being offered and that their needs are being met. For example, whether the products are sold transparently to the right people.

Stage 5 assesses the extent to which the business designs and reviews after-sales processes to meet customer needs and expectations. For example, whether the systems and controls for dealing with complaints and claims address the main causes of the problems.

The second element of proven responsibility is **effective control** and is a derivative of the liability element. Although an institution has a customer service area, it is not responsible for managing consumer protection risk issues. The effectiveness of the consumer protection risk management program falls within the risk management area, which evaluates all the controls throughout the product life cycle, from product development to the after-sales process.

The control of some consumer protection activities is assigned to the entity's operating units, for example: the marketing area, product development, information technology, customer service, among others.

The third element of proven accountability is **evidence**. In responsible entities, whoever assumes control of a consumer protection risk management activity provides evidence to show that this activity is effectively being implemented. When consumer protection risk management activities are being conducted on an ongoing basis, evidence is generated as a byproduct of the activity. In other words, having a risk management and behavioral compliance program will be evident to the supervisor, even if intrusive supervision is required.

Evidence can be formal documentation (policies, procedures or manuals) or even management information (internal or external communications, schedules or information system records) that can be used to demonstrate that risk management activity is indeed taking place.

Measures of demonstrated accountability should be based on a variety of factors specific to each financial service institution, including its size and legal nature, the nature of the specific products and services, risks involved for consumers, and the interconnections that may involve systemic risk. When the supervisor identifies that an entity is beginning to grow and undertake more complex operations, it should have the authority to make the entity eligible to be introduced into the usual cycle of intrusive supervision.

Finally, it is important to mention that the alternatives proposed in this document are not mutually exclusive.

That is, RSAs may choose to apply the consumer protection risk supervision model to those traditional firms and fintech with traditional and full licensing, which would fall under the on-site or off-site supervision program. On the other hand, firms or products relevant to the authorities that fall outside the perimeter may be served under the Demonstrated Accountability model.

Fintech companies under the Demonstrated Accountability program would not initially be part of the financial supervisor's on-site or off-site supervisory cycle. However, considering that companies outside the perimeter may be under the rules of a generic or crosscutting consumer protection supervisor, at any request of this generic supervisor, companies must disclose the implementation of the program. If they fail to do so or if deficiencies are found in the program, the supervisor must have the power to apply the corresponding sanctions.

The following are a few considerations that, regardless of the supervisory approach that its context and legal framework allows, the authority must consider in order to achieve an adequate supervisory scheme for fintech.

GUIDELINES FOR THE IMPLEMENTATION OF SUPERVISION STRATEGIES

As can be seen, some of these considerations are already part of regulatory frameworks, strategies and methodologies to some supervisors in the region. We would like to emphasize that the considerations developed arise both from what was expressed by the authorities in the surveys conducted by the Association, and from the experience of the Consultant and the advice of the WG.

Ensure Minimum Consumer Protection by Adapting And Developing Tools and Techniques to Address the Risks Associated with the Marketing of Fintech Products and Services

RSAs are at different stages in adapting to the challenges posed by the digitalization of supervision activity, but prior to this adaptation they need to understand the digital phenomenon in order to design appropriate supervision tools.

Consequently, the initial response by RSAs should be to set up internal multi-disciplinary working groups to understand the particularities of fintech and to adapt the supervision tools as necessary, and then to produce new tools and methodologies dedicated to supervision where needed.

- The creation of internal multi-disciplinary working groups (members of the supervision teams by activity, legal, IT, money laundering, risk, consumer protection) can be helpful in gaining a better understanding of fintech and determining the supervision strategies and tools to be applied to it. These groups should analyze the business models used by fintech, the risks associated with the consumer protection functions, and subsequently design regulatory and supervisory responses to those risks.
- Supervisors and regulators should use traditional monitoring tools and adapt them to address fintech service providers, especially in cases where legislation does not provide for the possibility of applying different tools or has resource constraints on their application. These tools include:
  - **Off-site assessments**: specific reviews of information files, advertising, pre-contractual and contractual information; holding regular meetings with financial institutions; questionnaires and requests for feedback; use of thematic assessments of consumer care functions or areas to assess compliance with legal requirements.
  - **Early warning indicators and risk indicators**: construction of warning indicators that will enable the anticipation of new risks arising from Fintech as they would with traditional financial products and services. Among the main early warning tools used by RSAs to anticipate new risks related to fintech are: social media screening, interviews with consumer representatives, industry research, surveys, and press releases.

    To design regular and reliable early warning tools, two sources of information are important as long as they are received through formal channels: complaint handling and

a hotline for informants (*whistleblowers*).

It is also recommended that risk indicators be developed from internal risk assessment workshops, internal teams and self-assessment tools for reported information, on-site inspections and operational risk assessments. Analysing the sites or apps being offered, and eventually testing of fintech products, allows supervisors to know, first-hand, the functionality of the product and the standards of customer services.

— **Supervision of complaints**: Complaints are a relevant indicator of the risks associated with a product or service and its supervision is still oriented towards traditional products. Complaints are classified by type of product, cause of complaint, financial service provider, etc. Therefore, there is a need to modernize the supervision process to support the identification of emerging issues related to digital products. With this in mind, we propose to clearly define the concept of complaint in order to adapt it to digital products and services. This way, an application or request submitted by a client to a financial institution not resolved within 24 hours must be classified as a complaint and the legal provisions provided in each jurisdiction for its attention and resolution will apply.

On the other hand, it is necessary for RSAs to build a database for handling complaints in the financial system. This centralized base is an app that organizes products, by-products, problems and sub-problems according to the regulation of each jurisdiction. Each client will enter his or her complaint into the system and the corresponding authority will send it to each entity so it can respond and the regulatory process foreseen for its attention can be followed, including the participation of the client's ombudsman, if this figure exists in each jurisdiction.

The authority would not verify the facts alleged in these complaints but may use the information to confirm and record a business relationship between the consumer and the entity. This way the supervisory authority monitors in real time the complaint source, date of filing, entity to which the complaint was sent for response, and the actions taken by the entity in response to the complaint. For example, whether the entity's response was timely and actions were taken in response, or whether the consumer did not accept the response and chose to escalate it to the ombudsman.

With this tool, RSAs can use complaint statistics as an important source of information for data analysis to identify trends and problems in the field. Thus, it is possible to conduct effective off-site risk-based supervision of entities, enforce financial consumer protection laws and write rules and regulations, as well as publish reports on complaints and share the information with other authorities and think tanks. An example of this tool can be found at *The Consumer Financial Protection Bureau*.[18]

— **Efforts to coordinate with other authorities** supervising companies and services outside the perimeter but relevant to the financial authority are essential. A key aspect of such activities is the joint assessment of requests, complaints and claims associated with digital products similar to those provided by financial institutions. The analysis of trends, technologies, innovations and the dynamics of competition in the financial market posed by these new offerors allows for prospective consumer protection initiatives.

— It is appropriate for RSAs to **review the functionality and efficiency of their regulatory frameworks for handling requests and complaints** in the new fintech product and service environment. In the regulatory review activities, it is a priority to examine the principles, procedures and the role of the authority against scenarios in which higher levels of inclusion may lead to an increase in the number of complaints.

A guiding criterion for such regulatory reviews

18 https://www.consumerfinance.gov/data-research/consumer-complaints/

should be to require prospective consumer protection analysis and early action by incumbents and new suppliers of fintech products. The supervisor with authority in this area must streamline this role by seeking greater efficiency in its processes, concentrating the activities on preventive supervision and monitoring the effective handling of consumer complaints by suppliers.

— **Specific information reports**: these are important tools that provide an overview of the digital products and services being launched on the market and their features. They should include the reporting of information security incidents considering personal data regulations. It will also be necessary to adapt the scope of the reports to collect data that inform about the entity's conduct towards consumers, such as new products offered in the period, products withdrawn in the period, changes in product terms and conditions in the period and retail product development.

— **On-site inspections**. Inspections will be required to enable access to fintech service providers' technology platforms regarding IT systems, cyber security, governance and business capabilities, including information security controls, cloud computing and robotic advisors. Specific plans will also have to be designed to assess fintech's relationship with third-party financial providers.

Supervisors must obtain the cooperation of supervised institutions to simulate, in real environments, the relationship between provider and client, according to the rules of each jurisdiction, playing the role of a virtual buyer who is allowed to operate the applications and verify aspects such as whether the general and pre-contractual information complies with the rules, the practical and operational aspects of the digital interface; whether the way of accepting the terms and conditions is technically adequate; whether the app complies with the legal requirements to monitor changes introduced over time, as well as to test different scenarios, profiles and use-cases, according to real situations identified in complaints filed by customers.

— Disclosure of data on complaints and their causes as well as how they evolve can be an incentive for constant improvement. This could contribute to making consumer satisfaction a relevant factor in competition among market players, which is desirable but not always possible due to the rigid rules of bank secrecy established in a number of jurisdictions.

- Regarding the creation of new tools dedicated to fintech supervision, supervisors must have the financial and technical resources to develop technology-intensive tools to facilitate their work. These include:

  — **Supervisory Technology (SupTech)**: Technological development can improve supervision by incorporating cutting-edge technologies into supervisors' procedures such as machine learning to detect quality problems in the information transmitted, such as data gaps, inconsistencies and errors, and automate data cleaning, consolidation, validation and quality control.

  Another approach is the development of APIs for supervised entities to report high quality granular data to increase comparability between entities, create new routes for analysis and reduce the burden of validating data at the aggregate level. The use of Distributed Logging Technologies (DLT) is also being used by security supervisors to reduce the complexity and costs of large reports. This could provide a high level of security and data integrity while maintaining aggregation costs and making data transfer more handy. The combined use of technologies such as ML, deep learning,

optical character recognition (OCR), natural language processing (NLP) and big data analysis allows supervisors to integrate analysis of multiple data sources and formats, which was impossible with traditional software.

— **Regulatory Technology (RegTech)** are innovative solutions introduced by financial service providers to meet regulatory requirements and improve automatic risk management more effectively and efficiently. Three general types of RegTech solutions have been identified: (1) those that help supervised entities to comply with their regulatory obligations, (2) those that help authorities to improve their market supervision and monitoring functions, and (3) those that help to reformulate current regulatory processes and systems. It is therefore recommended that the internal multidisciplinary working groups for fintech relate to the RegTech community in order to better understand their business models and developments, to perform technology tests in the fields of cognitive analysis to study web pages, machine learning applications that evaluate sets of documents and monitoring of social networks.

Increase Resources for Specialized IT Inspections and Keep Them Updated with the Changes in the Sector

As the digital transformation continues in the industry, IT risks are increasing, both in terms of probability and impact. The financial industry has particularly sensitive personal data and there is a history of well-documented cyber-attacks. Regulatory authorities continue to build and improve their regulatory approaches to IT and cyber security.

While supervisory authorities provide support in the areas of internal and external audit, a dedicated IT risk inspection team is needed for an intrusive assessment of IT investments, governance, and specialized controls to successfully mitigate these risks. This approach will address the technology challenges and changing business models associated with fintech.

Establish Units Dedicated to Behavioral Economics Analysis in Financial Consumer Protection

Digital environments are relatively new and have become very dynamic with the advent of new technologies (5G telecommunications, blockchain, cloud processes). However, human behavior in such environments has particular aspects that require detailed analysis. The application of behavioral analysis to the supervision of fintech has enormous potential to design policies and prove their effectiveness in practice by conducting randomized controlled trials, since consumer behavior may be different when obtaining financial products through digital channels instead of traditional channels. This recommendation applies to both supervisory authorities and service providers.

An example of this practice, on the public side, is the one carried out by the Australian Securities and Investments Commission (ASIC), which established a team dedicated to behavioral economics research, i.e. a research about the consumer and consumer policies. ASIC publications have provided support for implementing important regulatory details that benefit the consumer in the digital environment (e.g., screen size, time spent, order, channel, display) and can influence the attention and engagement that consumers show in the customer experience.

Consider Issuing Complementary Regulatory Materials Such as Guidelines, Best Practices, and Consumer Protection Principles

The issuance of regulatory supplemental materials such as guidelines, policy briefs, or warnings can be an effective monitoring tool for disciplining segments of fintech

and incumbent companies. These tools can be a valid alternative to changes in the regulatory framework, which may require a lengthy legislative process.

We recommend guidelines to be based on principles rather than prescriptive rules, and that they address specific issues in relation to digital problems, or that they modify certain existing guidelines related to traditional products to include the specific characteristics of the provision of these products and services through digital means.

Consider and Follow-up on the Evolution of New Channels for the Provision of Financial Services

Fintech product and service providers bring new and enhanced access opportunities using digital channels and omnicanality, but, in return, consumers may have less control in terms of initiating interaction with their fintech.

This is because the supply and distribution chain can be fragmented by the involvement of multiple specialists who are responsible for different pieces of that chain, leading to the retention of traceability of any information provided by consumers.

We have identified the following requirements that fintech service providers must ensure for the benefit of consumers:

- To have a secure key and encryption infrastructure, which ensures multiple standard encryption of data stored in the supplier's storage infrastructure and its supply chain.
- Guarantee information security and cybersecurity processes.
- Reveal the costs associated with maintaining the channel.
- Provide instructions for the use of the channel and guidance in the event of a channel failure.
- Increased channel automation should not eliminate the possibility of personal contact for customers purchasing certain products and services.
- Make sure the same channel through which the product or service was made available is used for its closure.
- Comply with current personal data protection and privacy regulations.
- Guarantee the traceability of all data in the storage infrastructures of financial suppliers and their supply chain.

When digital channels are used to link customers, new challenges arise in relation to AML/CFT risk management, because traditionally the identity of new customers is verified by analysts in a physical manner and using national identity documents.

In this scenario, regulation in several jurisdictions seeks to allow remote identification of customers, establishing the conditions to consider that such identifications comply with the due diligence requirements established in the respective AML/CFT regulations. This implies:

- Allow customer identification by video, which must occur in real time (live), and must be recorded with the customer's prior consent. Such records must remain protected.
- Use the national identification document presented by the customer, which must be accessible for a machine readability check. That is to say, suitable for the optical reading of particular sections of the identification document and to be able to decipher the characteristics of the encrypted information it holds.
  In addition, parallel identification measures should be taken separately from the identification document, such as verification of holographic features, clickable elements with visual effects, and the information should be cross-checked against official and online identity documents databases or private databases with the same kind of content.

These proposals may be limited by the absence of a coherent national cross-cutting regulatory framework that considers the following related aspects:

- Develop electronic identification: incorporate hardware and software components in national identification documents that securely store personal information and biometric characteristics with relevant potential for the incorporation and management of new customers.
- Explore and assess the use of distributed logging technologies (DLT) for the creation of a registration of individual digital IDs that includes traditional personal data, as well as biometric records, verified by government authorities, that will enable the expansion of the customer knowledge procedure in LAFT processes.

Consider and Follow-up on the Evolution of the Support Infrastructure that Enables the Provision of Financial Services. In Particular, the Infrastructure Related to Payment Systems

Currently, the most far-reaching work on the payment services segment has been carried out by the EBA and is aimed at ensuring that payments throughout the European Union are safe, easy and efficient; the regulatory outcome is condensed into the technical standards and guidelines of the Payment Services Directive (PSD2).[19]

The Directive has institutionalized the activity of so-called third-party providers (TPP), whereby the holders of a payment account expressly authorize a third-party entity, provided that it is duly authorized, to order payments on their behalf and/or to consult certain information associated with that account.

This way, the suppliers that offer clients a service will have a consolidated knowledge of the situation of the payment accounts that the client has with different entities, helping him/her with his/her financial planning; and there will be the suppliers that offer alternatives to the use of the cards, for the payment of the purchases that are made in electronic commerce environments. As a result, the traditional role that banking played as a single payment service provider will be opened up to new TPP players, which will weaken the degree of customer loyalty and the stability of transactional income.

The development of APIs as technical means that allow the sharing of resources between different open environments, for their massive use by third parties, promotes controlled access to banking environments. Banking, like TTPs, could also make use of APIs to provide services equivalent to those of these new competitors, differentiating themselves from them and offering higher value-added services.

In this new scenario, the authorities must make consumers aware of the consequences of their choices in the face of the greater range of options for completing transactions and financial operations so that they increase their precautions to avoid becoming victims of illegal actions and use the control tools offered by the institutions. Therefore:

- The incumbent entities as providers of Fintech products and services should endeavor to communicate to consumers the actual scope of the authorization they are giving to a TPP and to inform, in an explicit manner, the possible commercial use of their information beyond the provision of a particular payment service. Consumers should be aware that they may end up authorizing access to a volume of personal information that they would actually prefer to have kept private.
- A maximum-security environment should be provided for consumers when they choose to make electronic payment transactions, which requires measures to reduce the incidence of fraud and to ensure the continuity of payment services in order to enhance consumer confidence.

19 https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

FINAL COMMENTS AND UPCOMING CHALLENGES FOR THE AUTHORITIES

The considerations and recommendations made throughout this document provide a framework for regulating and supervising suppliers of fintech products and services from a consumer protection and conduct standpoint. These recommendations were developed considering the diversity of regulatory systems in the region and are not meant to prescribe standards given the constantly changing characteristics of the environment.

Whatever strategy the different financial authorities decide to adopt, it is necessary to ensure compliance with a series of tasks that are essential to consolidate an effective regulatory and supervisory framework for Fintech suppliers. Although these tasks are evident, the region's jurisdictions have encountered difficulties in enforcing them, and authorities are encouraged to design strategies according to the specific characteristics of their jurisdiction. These efforts include:

Understand the Risks Stemming from the Companies of Products and/or Services Resulting from Technological Innovations.

As regulators and supervisors, it is important that innovations are seen well in advance because fintech is present in all financial and securities market activities, and it is undesirable to wait until they are already in widespread use and have escalated in scope of use to be assessed or understood.

Therefore, one alternative is to develop an innovation center within the supervisory and/or regulatory body as a way for innovative companies to contact the authorities, with the intention of resolving their concerns and allowing the supervisor to learn about their ideas and the technologies these companies are developing. On the other hand, to obtain a vision of where both the financial services and the emerging risks are heading.

Generate Statistics and Identify the Scope of Fintech's Activity in Jurisdictions and in the Latin American Region, Both within and outside the Regulatory Perimeter.

One of the challenges of working with fintech involves the lack of statistical information to determine the importance and scope of new fintech business and to effectively track it (number of clients, products, distribution channel, customer service channel, geographic area of operations, etc.). This shortage of standardized and regular information hinders the development of supervisory tools and the assessment of potential risks.

For this reason, in order to obtain our own reliable statistics and to identify the scope of fintech's activity in each jurisdiction, we have proposed strategies to increase the authorities' knowledge of the fintech ecosystem, including those suppliers of products and services of this nature that are not part of its natural supervisory environment.

This can be achieved by implementing a centralized public electronic registry controlled by a third-party institution, such as a ministry or the equivalent of a chamber or registrar in charge of public record management, which significantly reduces any potential association that consumers may draw from a supervisory activity. For regulatory and supervisory authorities, this implies coordination with this third institution and the possible generation of regulations in this regard.

Review the Transparency of their Mandates: Overlapping Regulation and Lengthy Processes for Approving New Regulations Can Affect Consumer Protection.

It should be pointed out that the new regulation must be neutral with regard to technological change. This means that consumer protection rules apply equally to both digital and traditional delivery environments, and that they ensure that consumers are, and will continue to be, protected from the risks arising from switching-over to digital.

It is therefore necessary to analyze whether current consumer protection rules in each jurisdiction adequately protect consumers in an environment of innovative and technology-driven financial services.

Financial regulators and supervisors will need to consult with industry and consumer protection authorities to determine whether existing protections need to be improved or adapted, and equally important, to consider regulatory changes to assume supervisory and consumer protection functions for financial sector companies.

The Speed of Technological Innovation Contrasts with the Long Periods of time Needed to Recruit the Right Staff, Understand New Technical Needs and Approve New Training Courses

Supervisors must recruit staff in an open and transparent way, with high analytical and technological skills. At the same time, existing staff must be kept up to date. Supervisory authorities must also make greater use of technology to boost efficiency and effectiveness, given the increase in data from incumbents and fintech. Technology (SupTech) supports effective evaluation work and the constitution of analysis teams with better training in risk-based analysis and auditing.

Develop Regulation and Supervisory Methodology With a Risk-Based Approach to Consumer Protection and Achieve an Efficient Use of Work and Resources in the Areas Where a Significant Threat to Consumers Exist. Otherwise, if the Regulatory Framework Allows It, Adopt the Implementation of a Demonstrated Accountability Program Towards Fintech Companies Outside the Perimeter.

The development of the supervision model allows for thematic inspections to assess priority risks to consumers, for example, by focusing on a particular product, channel or activity. Thematic inspections focus on several fintech companies or incumbents within a financial activity. This allows for determination of whether the standards, at the industry level, are close to the level expected by the supervisor or whether there appears to be an industry-wide problem that may require policy changes, specific supervisory intervention, or compliance action to ensure appropriate change.

The lack of adequate mandates to enforce consumer protection, when foreign-based fintech provide products and cross border services, should be countered with increased cooperation among supervisory authorities and thematic inspections

Financial education projects should be incorporated through traditional institutions and fintech, both on their internet platforms and mobile applications. Within institutions, cultural changes are needed in the marketing and post-marketing of products to protect the financial consumer

Finally, financial authorities should continue to observe the emergence and development of new players and non-traditional business models, seeking to avoid regulatory arbitrage and ensuring that their activity takes place under consumer protection standards consistent with those of the traditional industry.

In summary, any regulatory and supervisory scheme for the conduct and consumer protection of fintech products and services must generate the right incentives for entities to comply with the following actions:[20]

- Act honestly, fairly and professionally in the best interests of customers and market integrity;
- Act with due diligence, skill and care in the best interests of clients;
- Avoid unwise, negligent or deliberate misleading of actual or perceived advantages or disadvantages of any product or service to a customer;
- Have and effectively manage the resources, policies, procedures, controls (on operational, technological and compliance risks) and staff training in order to comply with the prescribed regulation;
- Obtain from customers relevant information for the product or service requested;
- Make full disclosure of all relevant product information, including all fees and charges;
- Avoiding situations that could generate conflicts of interest;
- Correct errors and address complaints quickly, efficiently and fairly;
- Avoid exerting undue pressure or influence on a customer;
- Ensure that any outsourced activity complies with the prescribed regulation;
- Ensure that its policies, procedures or marketing practices do not prevent access to basic financial services; and
- Strengthen the protection of consumer information through cybersecurity risk management.

20 United Kingdom, Financial Conduct Authority, https://www.fca.org.uk/about; Irlanda, Central Bank of Ireland, https://www.centralbank.ie/about; Australia, Australian Securities and Investments Commission, https://asic.gov.au/

TERMS AND ABBREVIATIONS

Access to the same variety of products and services on all channels without losing quality	omnicanality
API	application program interface
Application	app
Automatic Learning	machine learning
Deep learning	deep learning
Asociación de Supervisores Bancarios de las Américas	ASBA or Association
Regulation and Supervisory Authorities	RSAs
Australian Securities and Investments Commission	ASIC
Inter-American Development Bank	IDB
Bureau Européen des Unions de Consommateurs	BEUC
Know your Client	KYC
Customer's ombudsman	ombudsman
Payment Services Directive	PSD2
Financial Education	FE
Push strategies	Push
Traditional Financial Entities	incumbents

European Banking Authority	EBA
European Insurance and Occupational Pensions Authority	EIOPA
Working Group	WG
Technology-based financial products	fintech
General Data Protection Regulations (European)	GDPR
Financial Institution	FI
Money Laundering and Financing of Terrorism	AML & CFT
Informant Line	whistleblowers
Memoranda of Understanding	MoU
Marketing	marketing
Natural Language Processing	NLP
Information Technology	IT
Peer-to-peer payment	P2P
Optical Character Recognition	OCR
Demonstrated Responsibility	accountability
Distributed Logging Technologies	DLT
Regulatory Technology	RegTech
Third Party Providers	TPP

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

Roberto Borrás
Consultant

ASBA
Marcos Fabián
Antonio Pineda
Ricardo Toranzo

BOARD OF DIRECTORS

Chairman
Paulo Sérgio Neves de Souza
Banco Central do Brasil

Vice Chairman
Jorge Alexander Castaño Gutiérrez
Superintendencia Financiera de Colombia

Director for the Andean Region
Ma. del Socorro Heysen Zegarra
Superintendencia de Banca, Seguros y AFP, Perú

Director for the Caribbean Region
Michelle Francis-Pantor
The Central Bank of Trinidad and Tobago

Director for the Central American Region
Ethel Deras Enamorado
Comisión Nacional de Bancos y Seguros, Honduras

Director for the North American Region
José Antonio Quesada Palacios
Comisión Nacional Bancaria y de Valores, México

Director for the Southern Cone Region
Juan Pedro Cantera Sención
Banco Central del Uruguay

Secretary General
Pascual O'Dogherty

ASBA MEMBERS

ASSOCIATE MEMBERS

Andean Region

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

Caribbean Region

Central Bank of Belize
Banco Central de Cuba
Bank of Guyana
Bank of Jamaica
Banque de la République d' Haïti
Cayman Islands, Monetary Authority
Centrale Bank van Aruba
Centrale Bank van Curaçao en Sint Maarten
Eastern Caribbean Central Bank
Financial Services Regulatory Commission, Antigua y Barbuda
Turks & Caicos Islands Financial Services Commission
Central Bank of Barbados
Central Bank of the Bahamas
Central Bank of Trinidad and Tobago
Centrale Bank van Suriname
Financial Services Commission, British Virgin Islands
Oficina del Comisionado de Instituciones Financieras, Puerto Rico

Central American Region

Superintendencia de Bancos, Guatemala
Comisión Nacional de Bancos y Seguros, Honduras
Superintendencia de Bancos y de Otras Instituciones Financieras de Nicaragua
Superintendencia del Sistema Financiero, El Salvador
Superintendencia General de Entidades Financieras, Costa Rica
Superintendencia de Bancos de Panamá
Superintendencia de Bancos de República Dominicana

North American Region

Board of Governors of the Federal Reserve System, USA
Office of the Comptroller of the Currency, USA
Federal Deposit Insurance Corporation, USA
Comisión Nacional Bancaria y de Valores, México

Southern Cone Region

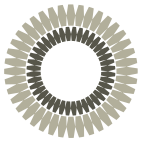
Comisión para el Mercado Financiero, Chile
Banco Central do Brasil
Banco Central de la República Argentina
Banco Central del Paraguay
Banco Central del Uruguay

Non Regional

Banco de España

COLLABORATOR MEMBERS

Banco Central de Reserva de El Salvador
Comisión Nacional de Microfinanzas, Nicaragua
Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, México




ASBA


IDB
LAB