Suggestions to adapt the banking regulatory framework to digital

While banks have traditionally been the key providers of financial services, the growth of the market and new technologies have helped the emergence of a new generation of non-banks in financial services. It is anticipated that these new entrants will play a greater role in the sector in future.

In particular, many non-banks such as big technology platforms have entered the market for retail payments and SME lending. These large tech platforms seek to enhance their access to consumer data and their ability to exploit that data for reaching and selling to customers. These new entrants differ from banks in that their main business is to take deposits and lend.

Customer expectations are also driving this change in financial services space. Despite the differences in the way banks and non-banks are regulated, consumers do not perceive the services offered to be of differing risk profiles.

As argued in the report "Bigtech banking"[1], when big tech companies enter markets with complex vertical value chains, they monopolize the layer or layers where they operate, entrench those monopolies by taking advantage of network effects, and extract value from all other layers by:

a) Vertically integrating with upstream and/or downstream companies;

b) Discriminating in favour of their own upstream/downstream businesses in their core platforms;

c) Leveraging data superiority to monopolize adjacent markets;

d) Intrusive data gathering; and

e) Maintaining control of key consumer gateways, operating systems and infrastructures.

Bigtechs have already entered financial services in the EU and are growing at a fast pace in the EU market, especially following the introduction of PSD2 regulation. Operating under payment institution and e-money licenses, they have access to banks' customer account data (e.g., Amazon in 2010, Luxembourg; Facebook in 2016; Ireland; Google in 2018, Lithuania; Facebook announcing the launch of WhatsApp Pay in Europe and already entered Brazil- https://www.finextra.com/newsarticle/36019/whatsapp-launches-payments-service-in-brazil?utm_medium=newsflash&utm_source=2020-6-15&member=101012).

These players are typically entering into payments, the gateway into a broader range of financial services. With huge customer data bases and large scale (millions of users, footprint), they are leveraging this - together with their flexible technology - to enter Europe, placing themselves at the customer interface.

[1] Padilla and De la Mano, 2018 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3294723

The entry of Big Tech players into financial services may have a significant impact on competition in retail banking. These platforms have large installed customer bases, established reputations, powerful brands, considerable earnings and unfettered access to capital markets. In addition, and importantly, they can leverage superior information about consumer preferences, habits and conduct—i.e. soft information. They control the shopping experiences of many consumers and recently the distribution and commercialization of many suppliers.

While this may appear to increase competition and benefit of consumers in the short term, within a few years Big Tech companies –or a single BigTech- may succeed in monopolizing the origination and distribution of loans to consumers and SMEs. Traditional banks that survive would likely become "low cost manufacturers," who merely fund the loans intermediated by the Big Techs. This would harm competition, reduce consumer welfare and potentially increase financial instability in the medium or long term.

After the COVID crisis, the provision of financial services through digital channels is only going to increase. We see the focus by European authorities on facilitating the adoption of e-technology, but we believe there is a lack of perspective regarding the changes in business models we need to accomplish to be successful in the digital context. If we want to adopt a platform business model, or move into adjacent markets, the whole platform will be subject to banking regulation.

Platforms are very successful because they deliver clear benefits to customers. They are also very helpful to business users, who can have access to a wider range of consumers. This is why the growth of platform providers has been exponential in terms of users and satisfaction.

However, banks are competing in this challenging space with a hand tied behind our back. Banks and non-banks are regulated differently, even when engaging in the exact same economic activity. When you want to evolve from a bank doing digital to be a digital provider of banking services, your digital activities are still treated as those of a bank. Competitively, this locks banks out of true competition in innovation of digital financial services.

In addition to the strategic evolution we need to make, we face regulatory barriers and increasing supervisory expectations that slow our ability to provide digital services at speed. We need to reconcile the possibility to test and assume risks (key for innovation) with the requirements of robust banking regulations (built to protect depositors).

The following paragraphs list in detail the barriers and examples that are often faced by banks and hinder the digital transformation of the financial sector, harming their capacity to respond to the extremely challenging competition dynamics:

Barrier 1: Governance requirements

We need to accelerate the development of the digital business within banks. To do so we need to provide them with the right talent, processes and governance, at the same level as our competitors have.

The solution would be to allow banks to create standalone entities to develop and accelerate technology and innovation businesses to serve the Group's banks at arms-length, as any other party in the open market.

The kind of activities that can fall under this approach are:

- The development of proprietary software and technology infrastructure and the provision of technology support to the bank or to third parties.
- Payment services, for individuals and companies, both cross-border and local.
- Financial solutions to simplify business management, trade or credit.
- Testing and digital activities or activities ancillary to the provision of financial services which have low material impact in the bank risk profile but are essential in innovation.

Today, governance requirements affect how these new entities can perform their operations when they are part of a bank, but not in non-banks. Governance requirements are set to ensure robust procedures across banks, including ensuring that their decisions are taken by the qualified persons, at the right moment and with the right elements of judgment. However, they are currently set in a manner that the criteria are those of the entire banking group.

Although different rules allow for a proportional approach, the governance framework limits the degree at which this proportionality can be applied to banking groups, especially if they are considered global systemic entities. The lack of clarity and the difference in criteria on how to apply proportionality to different kind of entities adds to this problem.

The reason is that both CRD IV and EBA guidelines on Corporate governance call for an institution-level governance framework:

CRD IV – Article 74

1. *Institutions shall have robust governance arrangements, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks they are or might be exposed to, adequate internal control mechanisms, including sound administration and accounting procedures, and remuneration policies and practices that are consistent with and promote sound and effective risk management. The remuneration policies and practices referred to in the first subparagraph shall be gender neutral.*
2. *The arrangements, processes and mechanisms referred to in paragraph 1 of this Article shall be comprehensive and proportionate to the nature, scale and complexity of the risks inherent in the business model and the institution's activities. The technical criteria established in Articles 76 to 95 shall be taken into account.*

CRD IV – Article 109

2. *Competent authorities shall require the parent undertakings and subsidiaries subject to this Directive to meet the obligations set out in Section II of this Chapter on a consolidated or sub-consolidated basis, to ensure that the arrangements, processes and mechanisms required by Section II of this Chapter are consistent and well-integrated and that any data and information relevant to the purpose of supervision can be produced. In particular, they shall ensure that parent undertakings and subsidiaries subject to this Directive implement those arrangements, processes and mechanisms in their subsidiaries not subject to this Directive, including those established in offshore financial centres. Those arrangements, processes and mechanisms shall also be consistent and well-integrated and those subsidiaries shall also be able to produce any data and information relevant to the purpose of supervision. Subsidiary undertakings that are not themselves subject to this Directive shall comply with their sector-specific requirements on an individual basis.*

EBA GUIDELINES ON INTERNAL GOVERNANCE

Title I – Proportionality

17. *The proportionality principle encoded in Article 74(2) of Directive 2013/36/EU aims to ensure that internal governance arrangements are consistent with the individual risk profile and business model of the institution, so that the objectives of the regulatory requirements are effectively achieved.*
18. *Institutions should take into account their size and internal organisation, and the nature, scale and complexity of their activities, when developing and implementing internal governance arrangements. Significant institutions should have more sophisticated governance arrangements, while small and less complex institutions may implement simpler governance arrangements.*
19. *For the purpose of the application of the principle of proportionality and in order to ensure an appropriate implementation of the requirements, the following criteria should be taken into account by institutions and competent authorities:*
    a. the size in terms of the balance-sheet total of the institution and its subsidiaries within the scope of prudential consolidation […];

Title III – Governance framework

Organisational framework in a group context

82. *In accordance with Article 109(2) of Directive 2013/36/EU, parent undertakings and subsidiaries subject to that Directive should ensure that governance arrangements, processes and mechanisms are consistent and well integrated on a consolidated and sub-consolidated basis. To this end, prudential consolidation should implement such arrangements, processes and mechanisms in their subsidiaries not subject to Directive 2013/36/EU to ensure robust governance arrangements on a consolidated and sub-consolidated basis. […].*

83. *The management body of a subsidiary that is subject to Directive 2013/36/EU should adopt and implement on the individual level the group-wide governance policies established* ***at the consolidated or sub-consolidated level, in a manner that complies with all specific requirements under EU and national law.***
84. *At the consolidated and sub-consolidated levels, the consolidating institution should ensure* ***adherence to the group-wide governance policies*** *by all institutions and other entities within the scope of prudential consolidation, including their subsidiaries not themselves subject to Directive 2013/36/EU. When implementing governance policies, the consolidating institution should ensure that robust governance arrangements are in place for each subsidiary and consider specific arrangements, processes and mechanisms where business activities are organised not in separate legal entities but within a matrix of business lines that encompasses multiple legal entities.*
85. *Parent undertakings and their subsidiaries should ensure that the institutions and entities within the group comply with all specific requirements in any relevant jurisdiction.*

How does this create an unlevel playing field for banks versus non-banks with which we compete?

Governance requirements reduce the flexibility that an entity within a bank group can apply to its digital activities, even when they are not creating significant risks to the entity (either because the volume is minor or because it is well separated).

These requirements make it very challenging for banks, and especially SIFIs, to innovate at the same speed as those players with flexibility, due to a simpler business model or because they are not banks. It is important to recall that very often the ambition of the entity is pure testing, without a long-term business plan. This testing is also critical for innovation.

These policies do not prescribe directly applicable rules, just principles, but entities are expected to develop frameworks to ensure their processes comply with the higher standards of robustness regarding risk control and governance models for those policies applicable to them.

Also, when the bank operates in multiple jurisdictions it is extremely complicated to take into account the different national regulatory requirements. The solution is often to raise the level of procedures to the stricter national requirements, so that every local subsidiary complies with its local requirement. However, this leaves most of the subsidiaries applying a stricter requirement than their competitors.

Policies that banks must always follow but that are not necessarily applied to other players are:

- Corporate policies and principles designed to meet regulatory and legal requirements must be applied to banks' digital entities.
- Compliance and conduct: Financial Crime; Regulatory Compliance (e.g. MIFID); New Products + Customer protection.
- Cyber security and T&O: Cyber and Risk technology; Sourcing and regulation; Data Management and Technology and Operations (incl. CIO, architecture).

- Internal Audit: Audit planning and execution, Monitoring of recommendations; and Escalation process and Reporting to Senior Management.
- Outsourcing and Third Party Management: Third-Party certification and risk assessment; Management of outsourcing and third-parties; and Cloud Transfers.
- Human resources: Suitability, Identification of Material Risk Takers (inc. Malus and Clawback); and compensation principles.
- Risk: Risk framework, appetite, models, systems and controls (incl. BCP, Fraud, EUC oversight, Tax strategy) and credit mandates.

This affects the way we organize different processes including:

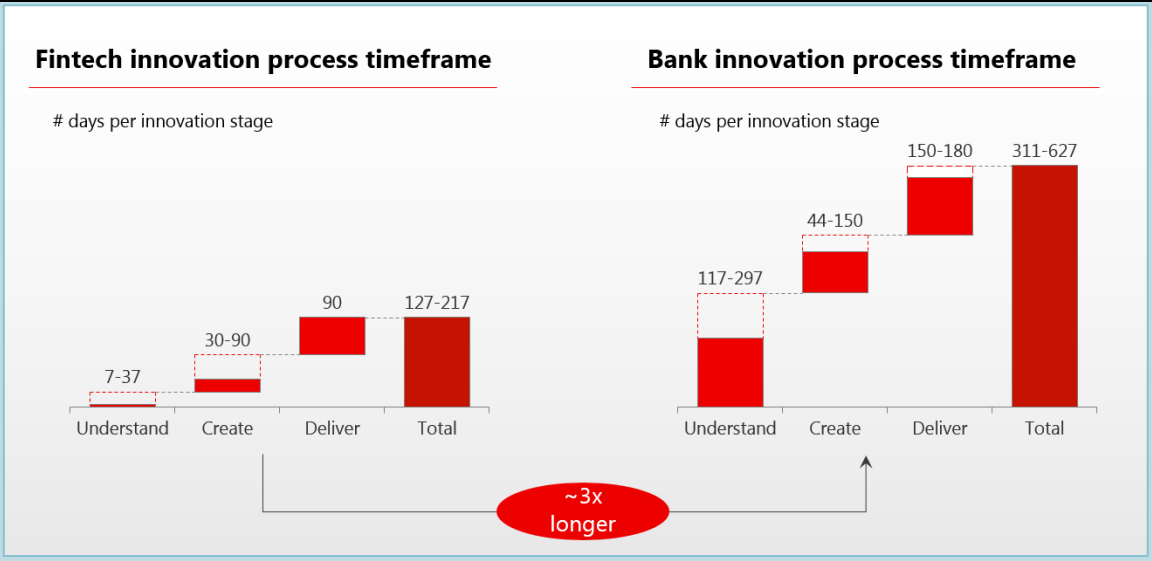
- product approvals;
- working with third parties and outsourcing services and functions;
- complexity in decision-making;
- testing products and new interactions models in the market;
- onboarding customers; etc.

This has many implications for the banks when innovating. One of them is that it increases the time-to-market.

We estimate that it takes a bank three times longer than a non-bank to complete all the required steps to launch an innovative idea. This is due to prudential regulations that require the bank to create and maintain complex internal legal and compliance processes, timeframes for securing regulatory clearance, additional protocols for engaging third party support and final governance protocols within the bank. Although clearance through a regulatory "sandbox" can provide clarity and reduce the timeframe, even with this process innovation still takes longer.

Table 1: Time to market for bank tech innovations	
Phase 1 – Understand the problem	To comply with internal, regulatory-driven policies, banks need to validate with the legal team ideas identified. (+10 days). If they want to test the ideas in a safe legal environment, the only option is to enter a "regulatory sandbox," which involve a wait of as much as 250 days.
Phase 2 – Create the solution	If a bank wants to work with third parties to create the technical solution, it has to comply with several outsourcing/vendor management rules that may limit or delay the options, depending on the level of readiness and contract flexibility of the counterparty (14 to 60 days). A bank is then required to build an additional layer of compliance over the third party supplier to meet its prudential obligations. Use of cloud service providers requires prior supervisory approval in certain countries.

Phase 3 – Deliver the solution	To validate the solution in the market, any new product launch or significant change to the product design requires formal approval from the Corporate Commercialisation Committee, extending the timing to launch the final product (+60 to 90 days).



How could the regulatory framework be amended to solve this?

We understand these activities – or the entities in which they are carried out - should not be subject to the whole bank Governance Model but should be able to apply proportionate governance infrastructure

The CRD already mentions proportionality, so we propose to just change the EBA guidelines to precise how proportionality can also be applied to entities with other corporate purposes.

EBA GUIDELINES ON INTERNAL GOVERNANCE

Title I – Proportionality

17. *The proportionality principle encoded in Article 74(2) of Directive 2013/36/EU aims to ensure that internal governance arrangements are consistent with the individual risk profile and business model of the institution, so that the objectives of the regulatory requirements are effectively achieved.*
18. *Institutions should take into account their size and internal organisation, and the nature, scale and complexity of their activities, when developing and implementing internal governance arrangements. Significant institutions should have more sophisticated governance arrangements, while small and less complex institutions may implement simpler governance arrangements.*
19. *For the purpose of the application of the principle of proportionality and in order to ensure an appropriate implementation of the requirements, the following criteria should be taken into account by institutions and competent authorities:*

a. the size in terms of the balance-sheet total of the institution and its subsidiaries within the scope of prudential consolidation;

b. the geographical presence of the institution and the size of its operations in each jurisdiction;

c. the legal form of the institution, including whether the institution is part of a group and, if so, the proportionality assessment for the group;

New letter:

(c'). in a Group or Sub-Group structure, the activity of each entity, taking into account whether it is an undertaking subject to a specific regulation.

d. whether the institution is listed or not;

e. whether the institution is authorised to use internal models for the measurement of capital requirements (e.g. the Internal Ratings Based Approach);

f. the type of authorised activities and services performed by the institution (e.g. see also Annex 1 to Directive 2013/36/EU and Annex 1 to Directive 2014/65/EU);

g. the underlying business model and strategy; the nature and complexity of the business activities, and the institution's organisational structure;

h. the risk strategy, risk appetite and actual risk profile of the institution, taking into account also the result of the SREP capital and SREP liquidity assessments;

i. the ownership and funding structure of the institution;

j. the type of clients (e.g. retail, corporate, institutional, small businesses, public entities) and the complexity of the products or contracts;

k. the outsourced activities and distribution channels; and l. the existing information technology (IT) systems, including continuity systems and outsourcing activities in this area.

l. the degree of development and maturity of their activities and services, in particular in the context of innovation and digital transformation life cycle. For those undertakings providing digital services at an embryonic stage, the governance framework should be proportionate to the risks embedded in their business models.

Title III – Governance framework

Organisational framework in a group context

84. At the consolidated and sub-consolidated levels, the consolidating institution should ensure adherence to the group-wide governance policies by all institutions and other entities within the scope of prudential consolidation including their subsidiaries not themselves subject to Directive 2013/36/EU. This adherence should be proportionate to their activities as stated in section 19l. When implementing governance policies, the consolidating institution should

ensure that robust governance arrangements are in place for each subsidiary and consider specific arrangements, processes and mechanisms where business activities are organised not in separate legal entities but within a matrix of business lines that encompasses multiple legal entities.

Barrier 2: Software deductions from capital

Banks are generally required to deduct software investments from their core capital, making these investments prohibitively expensive. Banks must pay for them with the most important resource they have to carry out their business - capital that has to be replenished as it is drawn down. This means software investments add to the cost of capital.

How does this create an unlevel playing field for banks versus non-banks with which we compete?

Non-banks do not have to deduct software investments from their capital. This creates an unlevel playing field for banks that is affecting both organic innovation and also the acquisition of fintechs.

When a bank invests in software, it needs to put aside similar level of capital to cover the CET1 requirements, in addition to the expense the bank actually made in the software. This increases the cost for banks in a moment where it is critical to develop technology (especially after COVID were many interactions had to move to digital).

The moment a bank acquires a fintech, this becomes especially visible, as the bank needs to fully deduct all the value of the software it acquired.

For every billion euros that a bank invests in software, with lending ratios of 20%s, if that investment were not deducted from capital, and with ratios of lending to individuals and for companies, it would support €36 billion in lending to individuals or €12 billion in lending to small and medium enterprises. Under current rules, that is credit that will never make its way into the economy to help people and business prosper.
U.S. banks do not face this requirement, one of the key competitive disadvantages European banks face when competing globally.

How could the regulatory framework be amended to solve this?

We very much appreciate that the European Commission has mandated the EBA to analyse under what conditions software should be not be deducted. There needs to truly be a significant capital relief - and as soon as possible, as time is of the essence given the massive shift to digital channels by our customers. The EBA's proposal under consultation is a simple and practicable approach based on prudential amortisation, but we believe that the proposed amortisation period should

be extended beyond 2 years to at least 4 or 5, to reflect that most software would not be negatively affected by resolution and that acquisitions processes can last more than 3 years.
The Covid-19 pandemic has shown us how important it is for all types of companies across the European Union , and this is also the case for banks , to have the appropriate technology systems in place to be able to react and continue providing services in the face of unexpected situations.

Barrier 3: Remunerations

EU banking remuneration regulations are a substantial impediment to recruit digital talent to EU banks. GAFAs and other tech companies, non EU-banks, start-ups and pharmaceutical companies around the world do not have such limitations.

This is mainly because of two items in EU banking remuneration regulations affecting the individuals which form part of the Material Risk Takers (MRTs) collective of a banking entity:

- The 1:2 limit on variable remuneration, which means that variable remuneration cannot exceed twice the amount of fixed remuneration for each individual. This is covered by CRD IV Art. 94.1.g)i) and ii) –and is not modified by CRD V, which is to be transposed into EU countries' regulations by the end of 2020-.
- The obligation to defer the delivery of a substantial part of variable remuneration for at least 3 years (minimum threshold to increase to 4 years with CRD V) and to pay at least 50% in equity instruments. This is covered by CRD IV Art. 94.1.l) and m) which are updated by CRD V to increase the minimum deferral period to be not less than four to five years and to exclude from deferral executives of entities which assets are not higher than €5Bn, as well as executives whose variable remuneration is below €50k.

How does this create an unlevel playing field for banks versus non-banks with which we compete?

Remuneration limits for banks are:

- Bonus caps: Bonuses for senior personnel, even in the Fintechs inside a bank perimeter, are capped at a certain percentage of basic pay by thresholds applied.
- Deferred bonuses: Material Risk Takers, a type of high-level employee identified in the regulation, receive bonuses in installments deferred during at least four years and can be subject to clawbacks.
- Supervisory approval and personal accountability: Senior managers (even in the regulated Fintechs within the perimeter) must be approved by the regulators (fit and proper).

These rules are a substantial impediment for to recuit digital talent to work for EU banks instead of BigTechs and other tech companies, non EU-banks, start-ups or pharmaceutical companies around the world, who do not have such limitations.

Digital talent is scarce, so this harms the capacity of European banks to access the best talent or increases the cost to recruit, as the limits on remuneration must be offset with other attractive features such as higher fixed salaries. When experts in AI, blockchain, biometry or other areas are needed to improve cybersecurity, fraud detection, digital consumer protection, banks' must devote more resources than others in attracting talent to maintain the highest standards of digital customers' security, safety and financial stability.

How could the regulatory framework be amended to solve this issue?

For entities within bank groups that provide digital services (including payments), the solution should be to amend article 109.5 of the CRD V, which states that those undertakings that provide certain services (including payment services) should be included in the scope of the governance requirements.

Additionally, to exclude payments institutions (a critical digital service), CRD V should be amended due to the inclusion within the scope of remuneration requirements of those undertakings that provide certain services (including payment services), on an individual basis.

For the rest of entities within the banking perimeter, and in the case that the Commission does not intent to remove the fix/variable 1:2 limit and deferrals, we think this problem for attracting digital talent can be addressed – even if partially - by carving out some individuals from the MRTs collective –and thus the limitations that apply to them.

In this regard, there are some proposals which have been put forward in feedback to various regulatory initiatives:

- Increasing the thresholds of entities within a banking group which would be exempt from the remuneration limitations in CRD IV –CRD V from FY2021- to those with up to €15Bn in assets, which in fact is what has been included in CRD V Art 94.4 – the exact detail will depend on local transposition, but the expectations are positive on this side.
- Exempting executives of non-regulated entities and of all non-EU entities within a banking group from the limitations above. It is unsure whether this has actually been the intention in CRD V when eliminating CRD IV Art. 92.1, but at the same time including modifications in Art. 109 which lead to doubt on this aspect. The banking sector is asking for clarification in this regard –and stating that the preference would be that all non-EU and non-regulated entities are excluded.
- Include in the "material risk takers" collective only employees involved in the generation of business and their control. This would require reviewing the qualitative criteria (i) in Art.3 of Commission Delegated Regulation (EU) 604/2014, and (ii) in Art. 6 of the current draft Regulatory Technical Standards on the criteria for staff identification.

Barrier 4: Outsourcing

The procedures that financial institutions must follow to approve new technological providers are not comparable to that of non-regulated entities. This includes banks and payment service providers.

Especially problematic are the following requirements:

- **Sub-outsourcing assessment** is one of the critical issues for the risk assessment, due diligence and oversight of outsourcing providers. Monitoring the sub-outsourcing chain **depends on suppliers** reporting on changes in their supply chain but also on our capacity to access and perform the due diligence of sub-service providers. Assessing sub-outsourcing activities through the **whole outsourcing chain**, which could potentially be long, might not be feasible in many cases.
- **Requiring unrestricted rights to audit suppliers,** which in certain cases become very problematic and difficult to apply in practice, since for example it will be subject to the supplier's willingness to allow this clause in their agreements. We believe this should only be required in case of outsourcing of critical functions.
- **Communication requirements**. Lack of clarity on what is considered "adequately inform competent authorities in a timely manner" regarding the planned outsourcing of critical services results in some jurisdictions in **procedures that de facto imply prior approval**.
- **Intra-group outsourcing**. According to the guidelines, intragroup outsourcing is subject to the same regulatory framework as outsourcing to non-group service providers. Although the guidelines recognize that "when outsourcing within the same group, institutions may have a higher level of control over the outsourced function, which they could take into account in their risk assessment," supervisory practice usually does not follow this case-by-case assessment, requesting the same cautions for all subsidiaries as third parties.
- **Perimeter delimitation.** There is not a consistent determination of which activities carried out by third parties are to be considered outsourcing, largely depending on the subjective appreciation of the local supervisor that may consider, for example, **any cloud solution as outsourcing.** Additionally, as supervision is executed at consolidated level, some subsidiaries are subject to the EBA GL even if their activity and risks are not financial in nature.
- **Critical or important functions.** The definition is not clear enough. This raises uncertainty and creates an artificially unlevelled playing field depending on subjective decisions.

As commented, the EBA guidelines on Outsourcing arrangements also extend their scope to the **use of cloud**, which could also be considered outsourcing and therefore subject to these requirements. Requirements set in some jurisdictions such as the need for a pre-notification become especially onerous for this technology increasing the time-to-market of cloud solutions compared to other non-regulated entities.

The **lack of clarity of the Guidelines** leave plenty of **room for interpretation in many requirements and for national "gold-plating"**. Sub-outsourcing may be strictly limited, which limits not only banks' capacity to work with third parties, but also conditions global activities which could be performed from global centers of excellence (which today is considered outsourcing).

Finally, the **EBA Guidelines set a demanding framework for financial institutions regarding the controls required on suppliers.** Compliance is very much achieved in arrangement negotiations which given the asymmetry of negotiation power with global Cloud Service Providers (CSPs) becomes a challenge, for example in introducing audit and access rights).

How does this create an unlevel playing field for banks versus non-banks with which we compete?

The procedures banks must follow to **approve new technological providers,** as well as the **flexibility needed to access cloud services,** are more rigorous than those applied to non-banks. **Regulatory requirements** create significant frictions in contractual negotiations between banks and Cloud Service Providers (CSPs). In addition, the **lack of harmonization** on the requirements that financial institutions have to meet across member states increases operating costs and hinders the scalability of services across Europe.

Examples of how this creates unlevel playing field are:

- **Communication requirements**. The approval procedure means that we needed to seek approval from the Joint Supervisory Team for a payments testing with 1000 friends and family group of customers. This implies clear delays in time to market (besides consuming resources from the supervisor at the same time)
- **Perimeter delimitation**. Considering any cloud solution as outsourcing makes that banks need to treat the same the outsourcing of functions such as the provision of lending as the outsourcing of the development of a new app for informing employees, if such app is hosted in a cloud. This multiplies the cost and the time consumption of any technology development that is supported by third parties.
- **Contractual elements required in outsourcing agreements**: According the EBA guidelines on Outsourcing, banks need to be able to include in their outsourcing arrangements clauses specifying e.g. whether or not sub-outsourcing of critical or important functions, or material parts thereof, is permitted; or ensuring full access to all relevant business premises (“access and information rights”) as well as unrestricted rights of inspection (“audit rights”) to both banks and their competent authorities, or to any other person appointed by them or the competent authorities. These specific requirements for the financial sector become difficult to negotiate and to be effectively applied in practice (e.g. in practice accesses to CSP data centers could be limited in number or frequency or penalized with an extra fee for additional accesses). This becomes specially challenging with SaaS providers. Much of the software used today is provided as a SaaS, which provides access to standardized services and leave therefore little room for negotiating their contracts. The fact that banks must negotiate specific clauses which are not required in other industries might end up limiting our access to these services.
- **Monitoring the sub-outsourcing chain**: EBA guidelines require financial institutions to perform the risk assessment and monitoring of sub-outsourcing activities through the whole outsourcing chain which will not be feasible in many cases. Again, this becomes a challenge for banks now that many software providers offer their products only as services (SaaS), relying on other CSPs to access cloud services. Banks would be required to analyse the risks associated with these fourth party providers. This requirement not only depends on suppliers e.g. to inform about changes in their supply chain – information that has commercial value in itself and that not all service providers may always be willing to

provide - but also on institutions being able to access and perform the due diligence of sub-service providers.

- **Data location restrictions**: Data localization requirements still exist in the EU, requiring financial institutions to include in their contracts with CSPs that the servers where the data will be located will need to be in Europe. This requirement means that suppliers who cannot provide this service, or who may not be willing to include such a clause in their contracts, are de facto excluded. This requirement does not apply to other sectors.
- **Restriction on sub-outsourcing chains in some regions:** In some jurisdictions it is not possible to carry out the so-called chain outsourcing, under which a subcontractor would entrust part of the activities performed on behalf of the supplier to further subcontractors. This restriction also applies to sub-suppliers (entities) belonging to one group.
- **Intragroup outsourcing:** The group intending to organize centers of excellence providing digital services for all entities across the group can be put at danger, which will harm the global digitalization efforts. More precisely, to perform Merchant services at group level, this activity is considered as outsourcing, so any additional outsourcing falls under the consideration of sub-outsourcing and create many inefficiencies.

The cost of compliance with these requirements is very high, requiring extra resources to meet all these obligations. Non-regulated competitors do not face these requirements.

In addition, supervision is Group-wide; all subsidiaries are subject to the EBA Guidelines even if their activity and risks are not financial in nature. All entities from a group must comply with the requirements and regime described for the delegation of services and functions (whether they are outsourcing or receiving services).

For example, if we provide different services from a global platform (e.g. technology and payment services) supervisory requirements may condition the way the business is organized. This is because, depending on how the provision of the services is organised - for example, by separating or not in different companies on the one side the technology services and on the other regulated activities such as payment services - this will condition supervisory requirements in the different geographies (requiring supervision not only of the activities related to the pure provision of technology services but also to the regulated activity of the company, even if this activity is already supervised in another European country, or whether the services provided are considered essential and could therefore require an authorization).

How could the regulatory framework be amended to solve this issue?

For entities within bank groups that provide digital services (including payments), the solution should be to amend EBA guidelines for internal governance to allow for proportionality, so the supervisory expectations should be reduced depending on the corporate purpose of each entity, its activities and the supervisory practices and expectations applied to those for similar competitors.

In addition, we believe that there is room for improvement in the regulatory framework:

- Reducing fragmentation at EU-level requires **establishing minimum baseline requirements avoiding gold-plating,** and **consistently harmonizing supervisory practices across jurisdictions**.

- The Commission should **mandate EBA to amend its guidelines on outsourcing.** We propose in particular the following amendments:
    - Sub-outsourcing: a financial entity should only be responsible for the direct relationship with its provider. Further responsibility to ensure that the sub-outsourcing complies with the agreed terms should lie within the company that decides to sub-outsource.
    - Communication requirements: it should be clarified that a notification process is sufficient and that a previous authorization should not be required.
    - The intragroup outsourcing should also be subject to lower compliance and reporting obligations than third-party outsourcing agreements. Intragroup outsourcing will in general result in lower risk to a group overall than outsourcing to third parties.
    - More clarity is needed regarding the perimeter delimitation of the guidelines (and particularly to the use of cloud), as well as to the consideration of services as critical or important. A risk-based approach needs to be followed focusing regulation on critical or important functions.
- The Guidelines should **be sufficiently detailed** to avoid differences in interpretation, and also **become mandatory for national supervisors** and **supersede other national regulations**.
- Regarding in particular to the use of the **cloud**, it is also essential to remove **data localization requirements,** allowing companies to store and process data wherever they choose. Ensuring the free flow of data, with appropriate security measures, is key for financial institutions to harness the benefits of cloud computing.
- The Commission should also consider a **specific oversight of third party providers (such as cloud providers) that become critical** for the financial sector ensuring that risks at system level are properly managed**.**
    - This makes even more sense considering the relevance of cloud infrastructures also for other sectors, and would be at the same time more efficient allowing companies to leverage the certainty provided by CSPs oversight.
    - Supervision of CSPs should be undertaken **once for the entire industry**, rather than requiring each individual financial institution to perform such checks, reports and controls over the same 4/5 CSPs. Initiatives such as the **promotion of certification schemes for CSPs** would also help to make this process more efficient, without reducing the level of supervision or the quality of the controls.
- At the same time, we welcome the initiative of the Commission to work on the development of **Standard Contract Clauses for cloud arrangements** which should support FIs in compliance with existing regulatory requirements. In order to become useful, SCCs should become binding for CSPs and could take the form of a **standardised addendum** setting minimum standards, and at the same time allowing enough flexibility for contracting parties to negotiate other clauses that could be specific of the service being contracted, the type of cloud, etc.

Barrier 5: Supervisory expectations

In addition to the regulatory requirements, banks need to ensure they meet supervisory expectations. Sometimes, innovations or internal measures require supervisory approvals before their adoption by the banks. Some examples are:

- When trying to **set up a global acquiring model for all of our subsidiaries**, providing services from one European country to the rest of the world, we encountered issues with some European national authorities who required us to set up branches in their national territories.
- Also, when trying to **provide global technological services from a technology company**, some supervisors expect to be able to have powers to supervise this entity, even if it is not based in its territory. With the supervision of this entity comes the capacity to supervise the parent company of such entity, which breaks the geographical limits of the business model and complicates the management of a cross-border group. We want to highlight here how much this contrasts with the lack of supervision of systemic technology providers, who can operate without this type of supervisory intrusion.
- **GDPR introduces additional uncertainty when using technologies such as AI or DLTs.** Their use may be limited depending on supervisors' interpretation of how GDPR principles apply to each use case (e.g. regarding how principles of data minimization, purpose limitation, or the right to object to automated decisions may limit the use of AI; or compliance with the 'right to be forgotten' or with accountability requirements in permission less networks regarding the use of DLTs). Divergent approaches taken by national supervisors increase the operational burden.

How does this create an unlevel playing field for banks versus non-banks with which we compete?

Banks who need to ensure supervisory approval can only move at the pace of their supervisors. Examples of how this creates an unlevel playing field are:

- **Operating models**: non-banks can organize their subsidiaries based on their own requirements, without interaction with supervisors. As such, they can provide technological services globally without further supervision. Requirements for banks such as the obligation to adequately inform competent authorities regarding the planned outsourcing of critical services to the cloud - which in practice may result in a de facto approval procedure - increase banks time-to-market and compliance costs compared to other non-regulated entities.
- **Loan origination:** non-bank players do not have the same limits regarding the documentation to be considered, the procedures, reporting, etc.

How could the regulatory framework be amended to solve this issue?

- For entities within bank groups that provide digital services (including payments), the solution should be the amendment to the EBA guidelines for internal governance to allow for proportionality. This could lower supervisory expectations, s depending on the corporate purpose of each entity, its activities and the supervisory practices and expectations applied to those for similar competitors.
- In addition, other regulatory measures should be considered:
    - **Reducing market fragmentation within the EU** requires **establishing minimum requirements that become mandatory for national supervisors to recognize, superseding other national regulations**. This becomes especially relevant for Cloud. The Commission should **mandate EBA to clarify its requirements**. Any **data localization requirements** should be removed, allowing companies to store and process data wherever they choose. The regulatory framework should remain **technology neutral,** follow a **risk-based approach**, and ensure a **level playing field for all industries.**
    - **More guidance is also welcomed** to provide **certainty about supervisors' expectations** about compliance with existing rules (e.g. GDPR, regarding the appropriate levels of explicability or the sufficiency of measures implemented to avoid discrimination when using AI), and to ensure the **same interpretation across the EU**. **A global consistent approach is needed** to ensure consumers and investor protection, and facilitate technology adoption in Europe.
    - Those activities whose regulatory framework states a specific supervisory process, regardless of whether those belongs to a banking group, should be excluded from the banking-approach consolidated supervision.
    - To assure the consolidated supervisor that the risks embedded in those undertakings which provide financial services, are prudently monitored, there would be two alternatives:

a) setting a regulatory framework for those undertakings which provide any digital service activity and the banking regulation allow the Supervisor to avoid the monitoring of those activities since they are already regulated y supervised according to their activity (which also means setting the supervisory expectations for those banking subsidiaries at the same level as their competitors, avoiding burdensome and time-demanding internal processes for banks) or;

b) establishing an option to isolate those activities outside of the banking perimeter (). U.S. financial groups may choose whether the prudential banking regulator should be heavily involved in regulating activities just because a bank does them; instead, U.S. groups can take these activities out of the bank's perimeter, subject to group-level regulation (from the Fed) and activity-based regulation applicable to the activity). European banks are at a competitive disadvantage because they do not have this choice.

We believe option "a" would be the best approach. Option b should only be put in place as a complement.

An additional option which could be implemented in the short term would be to develop **Internal exemptions within entities**: Since the aforementioned option would take time to be developed, an **immediate and temporary solution** to reduce the competitive disadvantages banks face in their path to enter into certain digital-based activities could rely on the creation of innovation spaces (like internal sandboxes) **within the banking group perimeter**.
This would be based on a regulatory statement, isolating the development of the innovative firms until a specific deadline or size, alleviating the regulatory burden in terms of internal governance, software, remunerations, outsourcing, etc, at the same time that its belonging to the banking perimeter **would allow the supervisors to have a certain degree of supervision** over those undertakings.
They would be different from the regulatory sandboxes already in place in that what we are proposing is internal and that does not have a specific deadline. Deadlines could be agreed on a case-by-case basis with the supervisors. The subsidiaries under this case would be governed the same as the non-banks subsidiaries performing similar activities and creating similar risks. This would allow banking groups to try out new solutions and also reduce the time to market of the innovative solutions within the bank's perimeter. This option would be linked with our proposal to amend EBA internal governance guidelines to include 19. l (new).

Contagion risks. A specific consideration for reputational risk

Banks' engagement in digital innovation should not put at risk the solvency of a bank nor create potential financial stability.

The solutions we have provided above are trying to balance the need to allow European banks to facilitate the development of digital finance and the capacity of supervisors to be able to detect if this is creating risks to the bank's solvency

As with other players in the digital ecosystem, trying to avoid any risk from digital activity, even low probability risk, is impossible. As with any other activity that banks perform, a risk appetite level needs to be set, under which we need to be able to innovate with fewer constraints.

A specific example is reputational risk. One could always say that, even in the case a fintech subsidiary is fully isolated in capital, liquidity and governance from a bank, in the case an uncontrollable event happens which have an adverse impact on this fintech's reputation, there is a risk that in the limit, the bank owning this subsidiary would be indirectly impacted by this.

Although we don't contest this connection, in theory, and we recognize it is not possible to fully isolate the bank of this potential impact, we believe that in practice the reputational risk that this business creates for the bank should also be assessed taking into account other elements such as

the size of the business, the number of customers, their nature, etc. and any mitigating action that the bank could take to reduce the impact of this risk.

The fact that reputational risk may potentially exist does not justify the treatment of a bank's fintech business as potential threats to a bank's solvency.

Risks of an unlevel playing field in digital financial services. What are the consequences for the economy?

The disparate treatment banks face creates two important sets of risks.

New risk - outside the regulatory perimeter.

Shadow banking

Fintech or new kinds of providers (such as the BigTech platforms) now clearly fall within the Financial Stability Board (FSB) definition of **shadow banking**. They are increasingly undertaking banking-like activities such as credit intermediation involving entities and activities outside the regular banking system, which are not subject to regulations similar to those applicable to banks. As an example, Amazon has expanded its presence in finance by offering short-term loans to small and micro businesses that sell on its marketplace. Since the launch of Amazon Lending in 2011, the company had surpassed $3 billion in loans by June 2017. In the 12 months up to June 2017, Amazon lent more than $1 billion to over 20,000 small businesses across the U.S., the U.K., and Japan with average loan sizes ranging from $1,000 to $750,000. Europe (excluding the UK) now has the fastest growth in lending by fintechs[2].

The issue here is not the creation of new sources of credit, which is welcomed when it is done responsibly and with appropriate oversight and risk management. But lending, like deposit holding, are core banking functions that are carried out in a very carefully managed system of rules and expectations that reflect the need for exceptionally robust prudential standards as well as the risks of pro-cyclicality inherent in credit provision.

By performing **liquidity transformation and maturity transformation**, creating **leverage** and conducting imperfect **risk credit transfer,** these firms are also generating new forms of risk, much of it outside the perimeter of current prudential regulation and supervision.[3] Regulators have worked hard over the last decade to prevent banking activity from moving outside the regulatory

[2] AltFi, Cambridge Centre for Alternative Finance. 2018

[3] Concerning the specific lending activity, the BIS (BIS and FSB report on Fintech Credit, Market structure, business models and financial stability implications) has found that Fintech credit gives rise to a number of challenges for regulators, such as potential deterioration of lending standards, increased procyclicality of credit provision, and a disorderly impact on traditional banks, for example through revenue erosion or additional risk-taking. FinTech credit also may pose challenges for regulators in relation to the regulatory perimeter and monitoring of credit activity.

perimeter into the “shadow banking” system. Despite these efforts, many financial activities now occur outside this perimeter.

Financial stability risks, related to lending activities

Moral hazard may be increased relative to the status quo because platforms follow an originate-to-distribute model with small or no stakes in the loans generated.

Adverse selection is also likely to increase, since platforms may have an incentive to price risk very low while searching for monetization in other markets. This could lead to a contagion effect in other players, which may need to reduce their lending margins to protect their businesses. In addition, given their rich data sets and superior technology, the new entrants may be able to screen out bad loans more effectively than the traditional banks. If that were the case, then the worst loans would be shifted to traditional banks, their investors and their depositors.

Monopolisation risk

In addition, the entry of digital platforms is also creating monopolisation risk (Padilla and De la Mano, Bigtech banking 2018):

Big Tech companies typically operate multiple platforms, so they subsidise business in different markets. Platforms operate in two sides and extract value from the interactions within a network and the data generated in the relationships with users. The relationship needs to be analysed in combination:

a. The side of the relationship more similar to the traditional one is where the consumer gets a service. But, instead of money, the consumer pays with data.

b. The business model of the platform is only completed when this data is monetized in a different market, where the platform provider can build a unique competitive position due to the data they extracted from other side.

This effect, called platform envelopment, can lead to market tipping or monopolization. The enveloping platform may be able to exclude other platforms as well as intermediaries operating one-sided businesses.

Platforms can also expand onto other businesses to acquire data. They succeed because they can combine data generated on various markets, which is difficult to replicate. We believe this can happen i.e. in consumer and SME lending:

a. Borrowers will likely transact through the platform used to compare products

b. Multi-homing will be even less common if purchasing decisions are delegated to digital assistants

c. Banks may find it difficult to offer differentiated services given that open data limits any informational advantage they might have enjoyed regarding their customers.

When they enter industries with complex vertical value chains, as the banking industry, platforms first dominate the layer where they operate, then use network effects, and finally extract the value generated in all other layers by vertically integrating, discriminating in favour of their own businesses, and leveraging their data superiority. This can happen in the banking business

The unintended consequences of an unlevel playing field

Risks can appear if banks cannot compete due to a stricter regulatory framework than necessary for the real risks that the activities create.

In this case, there could be:

Financial stability risks, related to bank disintermediation:

If banks are disintermediated from digital businesses, they will lose the information and relationships that they generate. Banks' capacity to deliver other vital services (i.e. lending) will be compromised.

The economy is dependent on banks' ability to lend and provide liquidity, especially in the EU. Lending margins are low and further shrinkage could compromise banks' ability to lend. If banks cannot power their lending with the digital business (and related customer relationship, relevance and knowledge gathering), the volume of lending might diminish. While a growing and deepening capital market may be able to compensate for falling bank lending, this will not compensate the risk of banks' declining capacity to lend. The entry of new lending providers, such as crowdfunding platforms, or the promotion of the capital market tools, is far from reaching the capacity to substitute banks.

Even BigTechs, with more capacity to provide credit, are not showing an interest in maintaining commitment over the cycle, as banks and specialised players do. The COVID crisis has shown this. For BigTechs, lending is just one more business line that can be abandoned or promoted according to the economic conditions, profitability rates or any other strategic reason. However, for banks, lending is the core activity and a reason to exist. They are committed to stay in both good and bad times.

The disintermediation of banks would make the economy much more fragile in an economic downturn.