Asociación Española de Banca

Fintech: A more competitive and innovative European Financial Sector

14th June 2017

1. Fostering access to financial services for consumers and businesses

1.1 What type of FinTech applications do you use, how often and why? In which area of financial services would you like to see more FinTech solutions and why?

Our members report us that they use an increasing range of FinTech applications, some of them developed internally and others in collaboration with third parties. The spectrum and intensity of the use of these applications varies from one bank to the other and includes new onboarding techniques, robo-advice apps for wealth and asset management or Insurtech services.

The ultimate objective of innovation in financial services is to deliver better and/or more affordable solutions to customers. This is something that FinTech solutions provided by digital players and banks can achieve, either working together or separately. Improvements can be obtained by enhancing the value proposition, reinforcing security features, opening new business lines, gaining efficiency or reducing costs, to name a few potential benefits.

When approaching this phenomenon, it is important to understand what types of FinTech exist, as this term covers a wide range of companies and solutions. If we analyse their relation with incumbents, these solutions can either compete with existing ones, unbundling the value chain, or enhance them by improving the existing offer and processes through partnerships. Another classification might distinguish between customer-facing services ("above the glass") or banking services enablers ("below the glass").

Customer-facing FinTech solutions offer multiple benefits, ranging from a better digital experience to better prices, and might potentially disintermediate the service provided by banks.

In relation to the Fintech solutions that many banks would desire to include in their processes –below-the-glass innovation, those related to RegTech are especially welcomed. Moreover, banks feel more comfortable approaching Fintech companies in a B2B model which is considered beneficial for both parties: Fintech startups can scale-up and adapt their technological developments to a real market need, and banks may incorporate

innovative solutions both in their internal procedures - by reducing costs - and in marketing and relationship with their customers.

Another area of interest is Fintech services to improve the current processing solutions in the payments or securities space (below-the-glass innovation). In this regard, it is of paramount importance to allow the testing and application of new technologies such as Distributed Ledgers or cloud computing, as we will highlight in the subsequent answers. Moreover, our banks welcome any FinTech solution that could optimise administrative processes such as reconciliation, forecasting, B2B procurement workflows, strategic advisory, fraud control, or alternative ways of funding, just to name a few.

That is why initiatives such as promoting a sandbox are essential to be able to develop and check the effectiveness of Fintech new solutions.

Artificial intelligence and big data analytics for automated financial advice and execution

1.2 Is there evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services (investment services, insurance, etc) and at what pace? Are these services better adapted to user needs? Please explain.

Yes. Automated financial advice is estimated to increasing their use in the short run given the following positive and clear benefits for the market:

- It increases accessibility to new segments of customers; Big Data analytics allows to reach more consumers given it provides a better picture of the user's needs. For instance, the robo-advisor model is ideal for customers with simple needs, or for small accounts that want to start to invest.

- It provides enhanced customer experience through mobile apps and increase transparency into investment options.

- It enhances the financial and investment knowledge of clients.

- From a cost efficiency perspective, it allows a reduction of operational costs once the initial developments are amortized.

However, the application of robo-advice is occurring at different speeds in the markets - being wider its use in countries like USA or UK - as a consequence of different factors. Probably the most important one is that although its use extends more across new segments as for instance *millennials* as digital native, there is still an important part of users who feel uncomfortable acquiring and using these services without any human support. We believe that the future development of these financial applications is mostly a combination of the two elements, human and artificial. In the physical world, this includes a specific model providing the automated tools at branch level: this way, the human is guided by automated

tools that enhance the consistency of the process, but respond to the customer demand of a close personal interaction.

1.3. Is enhanced oversight of the use of artificial intelligence (and its underpinning algorithmic infrastructure) required? For instance, should a system of initial and ongoing review of the technological architecture, including transparency and reliability of the algorithms, be put in place? (Please elaborate on your answer to whether enhanced oversight of the use of artificial intelligence is required, and explain what could more effective alternatives to such a system be.)

No.

From the point of view of how the supervision should be undertaken, we believe that it should consist of a combination of a set of minimal rules and ongoing assessment of supervisors. Internal controls and governance mechanisms can be designed to guarantee financial stability, along with a constant dialogue and interaction with supervisors to assess the performance of these financial tools –which should be on the other hand designed according to the banks' risk appetite framework and to the different internal policies and procedures and validated by the supervisor.

The use of AI will lead to models that evolve more frequently, as a consequence of the ongoing learning process. The oversight should not focus on the supervision of the algorithm that is at the end of the process, but on the **dynamics of the root artificial intelligence engine that has generated the algorithm**. For this, it is necessary that supervisors and regulators have among their human resources some specialists in Big Data and artificial intelligence to exercise proper oversight.

From the point of view of transparency, we do not believe that it is convenient to disclosure how the algorithms work; they are a source of competitive advantage for bank's business models and this could be put at risk.

There is a specific case concerning the oversight of robo-advice algorithms. We believe that it should be clarify that there are two main types of algorithms behind robo-advisors:

1. "**Profiling algorithms**" which are used to obtain a particular profile from the client through the information obtained from the knowledge and experience, investment objectives, investment horizon, etc. This process sometimes includes the suitability tests that MIFID regulates, in order to obtain the adequate information and profile clients correctly.

2. "Quantitative management algorithms" which are used to undertake decisions regarding the investment in a certain type of asset or portfolio.

Under the principle of same services, same rules, we believe that all participants should apply MIFID to profiling algorithms. The supervision of the "profiling algorithms" would avoid that clients perceive the same level of risk and quality of advice by robo-advisors taking different consumer protection measures. At the same time, the framework should be

ready for evolution and allow new ways to understand customer needs without a predetermined set of data. At this moment, all participants should be allowed to produce their analysis in a different manner.

In any case, regulations for AI should apply traditional players and new entrants given their relevance and increasing risk for the stability of the financial system.

1.4 What minimum characteristics and amount of information about the service user and the product portfolio (if any) should be included in algorithms used by the service providers (e.g. as regards risk profile)?

At present, there is a strict framework that prescripts the information that should be gathered by all providers of financial advice, which also applies to algorithms, namely financial market regulation (KYC, suitability) or GDPR.

Imposing specific characteristics or information requirements on algorithms could restrict the ability to innovate, create an unbalanced competitive environment or even lead to homogeneous approaches resulting in similar value propositions, hence excluding a part of the potential user base and, eventually, creating herd effects.

As long as the regulatory framework imposes rules on minimum information requirements (such as in MIFID or KYC), we support that there should be the same minimum set of requirements as it is the only way that a "level playing field" can be ensured. In parallel, in order to allow for innovation, there should be a review of how much information is needed to provide advice or any other service, with an eventual transition to a model where no minimum set of information is required. But this should be done for all players at the same time, without which there would be a clear disadvantage for regulated participants.

Information is of high value to cybercriminals and cyber terrorists. Therefore, measures to reduce the risk of data leaks and their consequences should be taken. These measures should not only come from regulation, but players engaged in Fintech activities (including financial institutions) should proactively take proper security and privacy measures to mitigate these risks. In this regard, all companies should be subject to equivalent supervisory requirements.

1.5 What consumer protection challenges/risks have you identified with regard to artificial intelligence and big data analytics (e.g. robo-advice)? What measures, do you think, should be taken to address these risks/challenges?

One of the main differences of these applications comes from the different way the relationship is established with the customer, which arises some challenges:

- The new channel must have a clear and understandable language and the way the information is gathered need to be very user-friendly in order to ensure the clients better understand their investments and their risks.

- Another challenge is how to structure the consent and processing purposes information requirements for protection of personal data in regards to big data and the evolution of what information can be processed and gathered. The client should know which information is being gathered and for which current and future purposes. However, we should take into account that, in many occasions, in the big data context, it is not possible to know all the future processing purposes from the very beginning. The obligation to inform data subjects about the specific processing purposes should be flexible enough to be compatible with big data.

- Lack of consumer awareness: In order to solve the customer understanding issues, some aids, tutorials and, when needed, human support, could be implemented by providers. Along with it, the compliance with MiFID II requeriments and GDPR will provide the suitable protection that consumers need.

Therefore, it is important that all players providing robo-advice respect these provisions, irrespective their nature or their geographic location. Although robo-advice can reduce the cost to provide advice, it is important that customers are equally protected and access high quality tools.

- Regulatory barriers: uncertainty about the impact of recent regulatory reforms (MiFID, IDD, MCD, PRIIPs) and how financial entities should apply them to automated advice business models.

Moreover, most AI services are built on a few platforms owned by big IT companies. An excessive market concentration could lead to artificially high prices, limited access to those services by some consumers and/or unbalanced commercial relations. Moreover, decisions taken by AI systems involve mechanisms and procedures, the rationale of which is difficult or impossible to understand by humans. Consequently, AI could be taking into account discriminatory parameters without humans being able to determine it.

In order to keep these risks under control, it is important to ensure the enforceability of current regulations on consumer protection, antitrust, privacy, discrimination, etc when using AI.

Social media and automated matching platforms: funding from the crowd

1.6 Are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding? Please elaborate on your reply to whether there are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding. Explain in what way, and what are the critical components of those regimes.

The existence of divergent approaches among national frameworks might fragment the internal market by limiting the provision of services across Member States and may also

create legal uncertainty as to what rules apply to which forms, potentially harming the growth of crowdfunding in Europe.

The Commission should foster the harmonization of regulation in order to minimize risks to both consumers and investors, and also to ensure a level playing field between financial and non-financial institutions (e.g. not all crowdfunding companies make the average default rate available to investors). Future regulation on crowdfunding should also aim to eliminate any potential asymmetries between financial and non-financial players (e.g. KYC and AML requirements).

Equity-based crowdfunding and crowdlending are regulated in Spain (CNMV), and in the case of lending or models involving payments services, authorization by the Bank of Spain is required. Consumer protection is at the heart of this legislation and discriminates between accredited or non-accredited investors. We believe this regulation offer more guarantees for both participants and investors than others across EU, although there is always room of improvement.

1.7 How can the Commission support further development of FinTech solutions in the field of non-bank financing, i.e. peer-to-peer/marketplace lending, crowdfunding, invoice and supply chain finance?

Rules should be put in place to establish minimum requirements, oversight and the reinforcement of the guarantees to crowdfunding investors that will give greater legal certainty to these tools.

Activity should be supervised on a daily basis. Services that entail similar levels of risk to those inherent to the banking industry (either financial stability, cybersecurity or investor protection) should have the same level of supervision.

In terms of consumer and investor protection, we believe that this activity must provide the same level of protection as the existing banking rules (MIFID II, Consumer Credit Directive or Mortgage Credit Directive). If we want a sound crowdfunding ecosystem to develop, retail consumers and investors should not bear more risks than they are willing to take as an informed decision.

The Commission could also contribute to spreading standards developed by the industry at national and European level, improving transparency and sharing best practices. This approach should aim at improving the information provided by users (both project owners and contributors), protecting contributors from fraud and ensuring an adequate complaint mechanism. An example of this is The Code of Conduct developed by The European Crowdfunding Network for its members.

1.8 What minimum level of transparency should be imposed on fund-raisers and platforms? Are self-regulatory initiatives (as promoted by some industry associations and individual platforms) sufficient?

At a minimum, the measures provided for in the Spanish banking legislation regarding consumer protection and transparency and conflict of interest should be articulated to protect users, especially retail investors. We understand that in this case self-regulation is not enough to cover all the necessary aspects in this matter.

Moreover, a clear allocation policy should be established in order to minimise information asymmetries:

- Investors should have the right to access the investment opportunities at the same speed than the institutional investors or the platform promoters.
- There should also make sure that no participant has access to more information than the rest.
- The promoter of a platform should not be able to invest in order to avoid the use of unbalanced access to the information.
- Every participant in a platform should know who is investing significantly in it.
- There should be the same transparency than for small caps issuances

On the other hand, as p2p and b2p lending platforms engage in lending, this type of platforms should be measured in terms of capital and reserves sufficiency by taking into account the principle of proportionality.

As mentioned before, self-regulated initiatives are often not sufficient to guarantee a symmetry of information between funding suppliers and consumers.

Sensor data analytics and its impact on the insurance sector

1.9 Can you give examples of how sensor data analytics and other technologies are changing the provision of insurance and other financial services? What are the challenges to the widespread use of new technologies in insurance services?

1.10 Are there already examples of price discrimination of users through the use of big data? Please provide examples of what are the criteria used to discriminate on price (e.g. sensor analytics, requests for information, etc.)?

**

1.11 Can you please provide further examples of other technological applications that improve access to existing specific financial services or offer new services and of the related challenges? Are there combinations of existing and new technologies that you consider particularly innovative?

Big data analytics and artificial intelligence are technologies with a great potential to further expand the access to financial services by lowering the complexity and the costs associated to certain advisory and credit scoring services, for example.

Other technologies might be used to reduce the complexity of interacting with financial

services providers. In this sense, behavioral biometrics is a promising field that will allow for a seamless user experience that preserves a high level of security.

Although digital platforms (including the so-called sharing economy) are not a disruptive technology in theirself, this innovative business approach makes use of available technologies such as the public cloud or mobile to reduce information asymmetries and expand markets to previously unserved or underserved segments.

We would also like to highlight the opportunity lying in the use of technology to improve financial literacy among European citizens. In this sense, informational dashboards fed by analytic engines and advisory and predictive models will let consumers and corporations take better financial decisions.

2. Bringing down operational costs and increasing efficiency for the industry

2.1 What are the most promising use cases of FinTech to reduce costs and improve processes at your company? Does this involve collaboration with other market players?

We believe that some of the most promising use cases are those related to DLT, Cloud services and Artificial Intelligence and Data analytics.

Cloud computing services mean clear improvements in terms of cost efficiency. Cloud computing already allows for greater scalability, more flexibility and shorter time-to-market when innovating. Cloud computing is also behind the recent APIfication trend, whereby infrastructure, platforms and data services can be offered to internal or external developers in an extremely convenient way.

In the case of AI, in addition to its benefits in terms of more tailored product design for customers, as processes are digitized, there is also an improvement in efficiency, replacing some of the less efficient tasks carried out by human (such a as servicing, contracting,..).

Distributed Ledger Technologies may also boost liberation of resources and system decommissioning mainly in middle office and back office processes. Reporting and Reconciliation processes are clear examples of this. Additionally, smart contracts that operate automatically will require minor manual intervention, which will translate into cost efficiency and at the same time more robust processes.

Biometric authentication technologies also are very much appreciated as they can accelerate all onboarding, digital signature and even KYC processes.

Another field where costs can be significantly reduced, and processes improved, is regulatory compliance and reporting. So-called Regtech can be considered as a subset of Fintech aiming at the resolution of exactly these issues through the application of big data analytics, AI, biometrics, DLTs or cloud computing, to mention some relevant technologies. This is a field in which certain start-ups, as well as incumbent technology firms, are actively cooperating with financial institutions.

Cooperation with smaller firms is often constrained by contractual complexity (especially when transferring data across borders or outsourcing infrastructure to public clouds). Regulatory and supervisory obligations often make excessively complex for banks to engage with innovative start-ups that do not have the resources or the expertise to develop risk control frameworks. EU-wide regulatory frameworks are desirable for this kind of cooperative approaches too.

2.2 What measures (if any) should be taken at EU level to facilitate the development and implementation of the most promising use cases? How can the EU play its role in developing the infrastructure underpinning FinTech innovation for the public good in Europe, be it

through cloud computing infrastructure, distributed ledger technology, social media, mobile or security technology?

The Commission's first and foremost role should be to develop a policy framework for innovations to thrive in the Digital Single Market for financial services. This extends to a regulatory framework that understands and embraces the profound transformation that the financial services industry is facing. This market-driven approach has of course certain shortfalls, hence the Commission should ensure that Europe's geostrategic autonomy and economic continuity is preserved.

The EU should be active in facilitating the development and implementation of digital financial technologies. It should help the European players to develop digital solutions, so that the EU is less dependent of technology providers from abroad, such as in the case of Cloud services or Cybersecurity.

Respecting the principles announced by the Commission of technological neutrality and market integrity, some of the measures in the areas identified above would be:

In cloud computing, the EU could play a role in:

- Adjusting the regulatory environment to the digital reality: we observe that the legal and regulatory constraints and the higher compliance risk derived from the use, management and storage of customer information constrain the adoption of cloud service models by a strictly (and comprehensively) regulated banking industry. It is vital to adopt measures to support the creation of a clear and consistent regulatory framework at an EU and Global level, and guaranteeing a proportionate risk-based approach to due diligence and contracts between the Cloud Servicing Providers (CSPs) and the banking sector.
  For instance, the financial regulation on outsourcing in the EU implies that banks should inform the financial supervisor ex-ante of each cloud project to be launched. This has to be done on a case by case basis, increasing time to market and impeding banks to innovate faster.
- Harmonising regulatory approaches across different jurisdictions. The variation in approach to cloud computing in financial services by various national regulators creates inefficiencies, particularly for institutions operating with a global presence and global customers.

Concerning DLT, the key is a favourable regulation in place in order to develop different projects with a safety net. There is also the need to have network effect. The authorities should be providing the framework to develop such nets. In our opinion, it is better to open a flexible framework for the technology, but without imposing general regulations that also include data protection (right to be forgotten, privacy).

The EU should create spaces for safe market testing of consumer-oriented innovations without incurring in the entire regulatory burden (prudential, data protection, cybersecurity). This “regulatory sandbox” approach would allow innovators to reduce

regulatory uncertainty and to test commercial viability before building a fully-fledged compliance structure. On the other hand, authorities would be able to learn and determine the risks associated with state-of-the-art innovations from early stages.

Cybersecurity is one of the key areas that the EU should strengthen, and regulatory sandboxes could also contribute to this goal. Moreover, the use of international recognized standards on cybersecurity would help to create at least a minimum baseline for all players in the industry. This new certification or labelling system should be principle-based. The NIS Directive is already pushing this idea but its scope does not include all relevant players in the industry or in other sectors too.

Finally, developing or acquiring the right digital talent and skills within the Commission is the best way forward for European policy making to keep pace.

2.3 What kind of impact on employment do you expect as a result of implementing FinTech solutions? What skills are required to accompany such change?

The digitalisation unavoidably brings a change in skills; some old jobs may disappear and other new ones will appear, the net effect not being necessarily negative. Moreover, fintech is likely to create greater dispersion in financial services-related employment as new players emerge.

Banks will need to implement large-scale career change programmes for their personnel, in order to respond in a flexible manner to the new digital world. Employees with specific competences on ICT, science, technology, engineering and mathematics are likely to be required not only by banks, but also by the rest of the firms, and surely by policy makers and supervisors too.

It is important to note that the current prudential requirements imposed to banks constrain the variable remuneration that an employee within a bank can receive; also affecting specialists who do not perform risk taking activities, but are crucial for the digital transformation, which makes very challenging to retain their talent (see response to question 3.1).

RegTech: bringing down compliance costs

2.4 What are the most promising use cases of technologies for compliance purposes (RegTech)? What are the challenges and what (if any) are the measures that could be taken at EU level to facilitate their development and implementation?

RegTech has the potential to transform the way financial institutions comply with the regulatory environment. Some of its most promising use cases are:

- The application of data analytics and the so-called "big data" can identify potentially high risk customers and can be used to reduce compliance risks in areas such as anti-money laundering. They also could make information more accessible and easily searchable to regulators. And in combining them with artificial intelligence,

could allow firms to reduce market risk through more precise modelling and forecasting of market trends and sentiments.

- Distributed ledgers can provide for the development of more efficient trading platforms and payments systems, as well as providing more transparent information sharing between financial institutions and regulators, which could allow firms to reduce operational costs and provide regulators with greater transparency and risk reduction.
- Regulators have pointed to cyber-risk as one of the most important threats to financial stability. The use of encryption can have the potential to reduce cybersecurity risk by creating another layer of security to data.
- The introduction of biometrics for the identification of clients, following KYC/AML/CFT legal requirements also may improve identity management and anti-fraud processes.
- Technologies such as robotics, sentiment analytics, or artificial intelligence to identify patterns can be used to automatically monitor compliance with the company's policies and procedures, laws and regulations by all members of the organisation by contributing to a better compliance of the customer protection processes.

One of the challenges related to the introduction of Regtech is how to reduce the regulatory uncertainty (due in part to the still unfinished regulatory agenda) and to harmonise the procedures and standardize information demanded by different authorities, which makes regulatory reporting extremely burdensome today.

Another challenge is the future development of RegTech itself; as it is quite an immature market, it is hard to predict how the ecosystem will evolve. This might lead to doubts when outsourcing in RegTech companies, as there is still uncertainty regarding their efficiency and acceptance by regulators. Currently, there is a promise to leverage existing systems and data to produce regulatory data and reporting in a cost-effective, flexible and timely manner without taking the risk of replacing/updating legacy systems. However, this is only a first step towards a more ambitious vision on data-led dynamic regulation. Big efforts are being made on predicting compliance problems through the use of advanced dynamic anomaly and pattern response systems, prediction markets alongside statistical systems, and automated surveillance.

Recording, storing and securing data: is cloud computing a cost effective and secure solution?

2.5 What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services?

The current regulatory / supervisory framework governing outsourcing is an obstacle to the greater use of cloud computing services by banks. It is not updated since 2006 and not adapted to the cloud computing technology. In this regard, we welcome the recent launch of a public consultation on draft recommendations on cloud outsourcing.

Data controllers need to fully understand and be accountable for the data and associated risks (cross border, data flows to subcontracted third parties, etc) when they use the services of cloud servicers. Moreover, cyber-security is one of the most important priorities with regards to the use of cloud computing services. Cyber-attacks are a constant threat nowadays, and the security measures provided by cloud computing services providers (CSPs) must stay up to the necessary level of security standards. Security measures by CSPs should be as developed as financial sector companies expect and need them to be.

Another element is the lack of harmonisation in regulatory and supervisory approaches across different jurisdictions. Some institutions have started the migration of banking information to the cloud and they face there are not a specific framework under which this should operate. This is leading to some uncertainty among banks and an extra effort from the side of supervisors. Currently the response has been different depending on each local supervisory authority that has issued different requirements. It has led to situations such as that a solution that has been developed in one country and migrated to the cloud under the supervision of a determined national authority cannot be used in other countries, as it should be tailored to different requirements.

Here, again, we see the need for supervisors and regulators to get staff with knowledge on this technology in order to allow for informed decisions to be taken at supervisory and regulatory level.

In the case of Spain, Circular 2/2016 Bank of Spain, deriving from EU 2013/36/EU and 575/2013 Regulation, is an obstacle to a wider and more agile use of cloud computing technology, as cloud projects approval could take up to a month or even longer if there are international data transfers.

On the other hand, there is a need to speed up cloud adoption in the EU. There are also certain overlaps between ECB/EBA and data protection authorities as regards how banks process personal data and safeguards measures to be taken at this respect.

Does this warrant measures at EU level?

We believe that the European Commission could focus on efforts that support the creation of a clear and consistent regulatory framework at an EU and Global level. The variation in approach to cloud computing in financial services by various national regulators creates inefficiencies, particularly for banks operating with a global presence and global customers.

The European Commission should instruct the European Banking Authority (EBA) and the European Network and Information Security Agency (ENISA) to prioritise harmonisation across jurisdictions through the fast adoption of guidelines or an update of existing guidelines to ensure a common approach by regulators/supervisors regarding procedures and methodologies and cloud projects approval. A positive step would be to develop some internationally recognized standards for the sector, taking into account the already existing standards, and that the providers are required to reach this as a minimum level. The work can be done together with standardization agencies (such as ISO) that could later certify

that the providers reach at least the minimum conditions, including cybersecurity and privacy.

In terms of cyber-security, regulators need to be aware of risks arising from weak IT systems. In this regard, cyber-security cannot be treated nor regulated with proportionality criteria. Cyber-attacks must be prevented not from the largest companies, but from all of them. As the European Parliament stated in its recently-approved FinTech Report, "a connected system is only as safe as its weakest element", and due to the interconnectedness of the financial sector, it will be critical that all CSPs ensure the same level of cyber-security.

Moreover, the Commission should continue its positive work under its Free Flow of Data Initiative to remove unnecessary data localisation requirements, except where necessary for legitimate public interest reasons.

2.6 Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with?

Yes, in general terms, but it varies widely between cloud services providers. The big cloud services providers already meet the security requirements established by international recognized standards such as ISO 27001, NIST, PCI, and they even have SOC2 reports based on SSAE 16 to assure compliance.

The doubts about data localisation and privacy – since most of the cloud services providers come from outside the EU with different regulations – hinder their use.

Banks have to take steps to demonstrate that a regulator can exercise a right of effective access to data and to the business premises of service providers processing that data. However, the physical access to premises hosting the cloud infrastructure is often a point of tension in negotiations with the cloud services.

More broadly, banks must demonstrate that they are using service providers that commit to co-operating with regulators in connection with the oversight of the cloud arrangement. Were cloud services providers required to comply with standards that foresee these requirements, it would be easier for banks to comply with supervisory demands, as these terms would not have to be negotiated in every individual contract.

Should commercially available cloud solutions include any specific contractual obligations to this end?

Cloud solutions are a special type of IT contract that blends technology provisions and outsourcing services. Therefore, contracts governing cloud services should be drafted in accordance with the regulation on those fields, in addition to the applicable financial regulation.

If the EBA/ECB undertake the homogenisation process of the different requirements needed for the financial sector (including cybersecurity, data protection, physical security, business continuity, right to audit, etc), then commercially available solutions should

include all the parameters in the contracts. In this regard, we expect the discussion around the recent EBA draft recommendations on cloud outsourcing to improve the harmonization within the EU.

Hence a common regulatory framework should be developed so as to facilitate compliance with a commonly understood set of minimum requirements to operate in Europe, translated into a core of minimum contractual arrangements to be included in all contractual relationships between CSPs and their users, certainly:

- That all data stored in CSPs' infrastructures are located, treated and processed in the EEA zone, including when cloud computing services are subcontracted.
- That CSPs allow their users to undertake every operational or technological controls required by internal policies and processes, as well as every requirement regulators may ask in the future.
- That all data stored in CSPs is encrypted.
- That CSPs comply with all data protection and privacy rules.
- That CSPs obtain and maintain every certification required by specific regulator or body governing cloud computing services.
- That CSPs ensure cloud users to undertake continuous monitoring activities whenever necessary, as well as virtual or ongoing audit.
- That CSPs must report any IT or cybersecurity incident, in particular when the data breach could be identified as that pertaining to a specific client, to both their clients and their supervisors, and that they will ensure that incident reporting deadlines are met by their clients.
- That CSPs have a business continuity plan for every client, so as to ensure the latter are able to switch providers whenever they deem necessary.
- That users of cloud computing services hold the right to extract data anytime.

Disintermediating financial services: is Distributed Ledger Technology (DLT) the way forward?

2.7 Which DLT applications are likely to offer practical and readily applicable opportunities to enhance access to finance for enterprises, notably SMEs?

Some of potential applications of DLT to financial services are those listed in the Commission consultation. There are numerous other potential applications too, that have been widely publicised, for example, cross-border Trade Finance, Supply Chain Finance, Bank reference data or Micropayments, B2B and P2P payments instantaneously settled, that we believe they can impact enterprises and especially SMEs, not only in terms of access to finance, but also in the way they do business.

2.8 What are the main challenges for the implementation of DLT solutions (e.g. technological challenges, data standardisation and interoperability of DLT systems)?

It is extremely difficult to assess thoroughly the impact of the blockchain/DLT in financial institutions services. It seems clear that such new technology would have a strong impact on costs in technology renew and it would lead to a deep reshape of training, processes, standards and business models.

For such reasons, we think that the following main areas should be addressed:

- The Governance framework for migration to the new technology at industry level (rules governing the interaction of participants, capital requirements, conduct of business rules, risk management processes, remuneration model, reversibility rules in case of mistakes or frauds)
- Issues related to privacy (for financial services the client and transaction data's privacy is of paramount importance) and the identity of participants;
- The technological needs (scalability and interoperability);
- The definition of the standards to be used for the different business areas;
- And above all the definition of a general legal framework (dealing also with legal enforceability of smart contracts).

2.9 What are the main regulatory or supervisory obstacles (stemming from EU regulation or national laws) to the deployment of DLT solutions (and the use of smart contracts) in the financial sector?

Although we recognize the potential of this new technology, we share ESMA's view that any regulatory measure for DLT would be premature in the short time. At this stage, a cautious approach on the DLT technologies is advisable, since it is not completely clear yet the impact of these technologies on banks' services.

Having said this, we consider that the potential uses for DLT are numerous and diverse and consequently, the adoption of a "one size fits all" regulatory framework for DLT wouldn't be effective. Hence, any regulatory-approach should focus on the financial activity that utilizes DLT, and not only on the specific technology.

As in other areas mentioned in this Consultation, we think that divergent regulatory approaches to DLT across the different jurisdictions may hinder the adoption of DLT in an optimally beneficial way. To this extent, cooperation and international harmonisation to enable an effective and facilitative DLT framework would be desired.

Some of the main obstacles in order to enable projects to develop further are:

- The legal definition of settlement finality
- The geographical location where data is physically stored
- The regulatory definition and treatment on cash on the ledger

Outsourcing potential to boost efficiency

2.10 Is the current regulatory and supervisory framework governing outsourcing an obstacle to taking full advantage of any such opportunities?

As we have already mentioned, there is a need to update the framework on outsourcing, so that it is adapted to the cloud computing technology to take full advantage of the benefits derived from the use of the cloud and in this regards, we welcome the recent launch of the EBA's public consultation on draft recommendations on cloud outsourcing

Moreover, there are certain cases where the supervisory practices can act as barriers too, especially when the service to be outsourced could be considered essential. Regulation imposes a burdensome process for financial outsourcing approval and there is a need to bring efficiency to this process

2.11 Are the existing outsourcing requirements in financial services legislation sufficient?

Yes, although they have to be updated together with the desired harmonisation of criteria among the different Member States and the correction of overlaps between the data protection authorities (DPAs) and the ECB/EBA regarding data use.

2.12 Can you provide further examples of financial innovations that have the potential to reduce operational costs for financial service providers and/or increase their efficiency and of the related challenges?

- Blockchain use cases
- Digital Identity solutions. Banks as trust provider. Compliance obligations related to integrity (i.e. KYC, AML, etc…) could be more efficient if there were a regulatory framework that allowed public/private institutions (indistinctly) to provide KYC services. This framework should include rules, data standards, and control & auditing systems. This type of service would reduce the red tape of necessary duties to perform due diligences and ensure that technologies and providers meet all legal requirements. In this regard, technologies already mentioned in this consultation, such as big data or cloud, could help to improve processes.
- Artificial intelligence (AI) and Data to enhance customer segmentation and be able to provide better customer service and products (for example, contact center tools or lending engines).

3. Making the single market more competitive by lowering barriers to entry

3.1 Which specific pieces of existing EU and/or Member State financial services legislation or supervisory practices (if any), and how (if at all), need to be adapted to facilitate implementation of FinTech solutions?

The new digital era is transforming the way banks do business. However, banks can not embrace this change if regulation does not adapt to the new digital environment with the appropriate changes and speed. This is important because, above all, this means carrying out an effort by regulators and supervisors to shorten deadlines and minimize bureaucracy to allow the adoption of new technologies with the minimum barriers.

A holistic approach to understand changes in business is needed to be adopted by regulators and supervisors, which requires effort in terms of human resources, training and technology. Also, in order to foster innovation and better understand its benefits and risks, it is crucial that the public sector invest in secure places where incumbents and new entrants could try the new technologies (i.e. sandboxes) with minimum costs for all.

In terms of specific regulation, we believe that much remains to be done in the following areas (not covered specifically in other sections of this Consultation):

- Software and digital talent:

Banks willing to become digital need to invest heavily in two critical areas: software and digital talent. However, the prudential regulation in force penalizes both areas in different ways and impedes technological neutrality.

Software has become a key asset for business models of banks that want to undertake digitalisation. Software investments are penalized in the case of EU-based banks, where its capital treatment as an intangible asset causes it to be fully deducted from Core Equity Tier 1 (CET1) when calculating capital requirements (Article 4. CRR). This undoubtedly represents a disincentive to invest in technology and, in turn, an element of clear competitive disadvantage for European banks vis-à-vis their peers, e.g. Americans, and other new entrants.

On the other hand, the recruitment and retention of digital talent in banks is also affected by European prudential regulation (CRDIV), which limits the variable remuneration that an employee can receive. This limit hinders banks' ability to attract and retain digital talent for which banks compete against players that are not subject to these rules.. To solve this issue, remuneration rules should be applied in a proportional manner such that non-significant subsidiaries of banking groups can be assessed on a stand-alone basis. Furthermore, an exception (waiver) to remuneration caps should be included for digital professionals and the founders and management teams of acquired start-ups. These amendments could be introduced in the revision to the Directive (CRD5), and should be implemented consistently across jurisdictions.

- Data:

Equality of conditions in the use of data for the provision of financial services must be achieved both at European level, for all types of financial enterprises (banks and non-banks), and between European and non-European firms.

The European rules or initiatives that regulate the data and their exchange (PSD2, GDPR and the Free-flow of data initiative) should be developed in a manner that is balanced to all market participants and guarantee that players are allowed to extract value from the work they perform with data, while preserving data protection and the privacy rights for consumers.

On the other hand, stricter European rules should not inhibit EU firms' ability to innovate, to operate dynamically, to use innovative data services and to direct services to targeted market segments if their competitors from outside the EU can serve European customers without similar restrictions.

- Electronic identification:

Digital identity frameworks are currently not sufficiently developed and regulatory fragmentation across Europe regarding digital identity remains a big obstacle to reap the benefits of the digital financial services. Therefore, the development and proper implementation of new digital formulas, fast, simple and safe that allow the identification and remote access of customers by electronic means should be promoted.

The Electronic Identification and Trust Services Regulation (eIDAS Regulation) creates an interoperability framework for the national eID systems to be recognized by public bodies across the EU. However, it leaves it up to Member States to define the terms of access to the online authentication of eIDs for the private sector. This gap should be addressed by creating a clear framework for the private sector to use national eID systems. This framework should clear out the liabilities in case of vulnerabilities, misuse, fraud, cyber attacks caused on whatever entity is acting as the central identity holder..

There is also a need to ensure a consistency in the implementation of the 4th AMLD across Member States due to, in relation to electronic identities; some EU Member States allow the use of non-face-to-face identification for customers by means of videoconference, while others do not.

Alternative methods for e-identification (such as biometry) should also be allowed

3.2 What is the most efficient path for FinTech innovation and uptake in the EU? Is active involvement of regulators and/or supervisors desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants?

Yes. Currently there are asymmetries and unbalances between new entrants and banks, and also between countries. Regulators should try to create a level playing field, namely by reducing restrictions applicable to incumbents to the same level established for new

entrants, in some cases, or by ensuring the new Fintech firms undertake their activity with the same level of requirements in terms of transparency and consumer protection.

As the Fintech world evolves at a high speed, regulators should also monitor the emerging risks and take action when needed. Moreover, the financial innovations help to improve the quality and variety of banking services, complete the market and improve allocative efficiency. Therefore, given its expected gains, it is necessary to create a framework that enables innovation to reach European consumers. In this strategy it is necessary to open a dialogue and collaboration between the industry and the supervisory agents. The active involvement of the various private providers, regardless of their size or nature (i.e. banks, technology companies, service providers or start-ups) should be allowed. This conversation will lead to a learning process where all stakeholders will be able to understand the needs and requirements of each other, allowing them to better manage the new types of issues that might arise in the most efficient manner, while preserving financial stability and ensuring customer protection.

We believe one of the most efficient ways to achieve this is, undoubtedly, the development of Regulatory sandboxes, which are secure places for experimentation and testing that provide very useful information not only for participants, but also for regulators and supervisors to monitor innovation in the financial system and increase a healthy competition, ensuring an ongoing dialogue and collaboration between the industry and the supervisory agents, as the technological innovation runs very fast.

Finally, although regulation is a key part to allow financial entities to embrace the technological change, in many areas may be more appropriate the developing of standards and tools.

Regarding the issue whether the authorities should foster **competition or collaboration**, both approaches are desirable and should coexist, as FinTech solutions can either improve current processes or provide new products and services.

FinTech companies, both incumbents and start-ups can also be supported through non-regulatory initiatives in a case by case approach, such as:

- tax optimization of startups (costs/employees/insurance etc.)
- simplify and support the way of financing (crowdfunding, venture capital, private equity, etc.)
- simplify and support forms of cooperation with organizations (corporations)
- support EU funds/cooperation countries with organizations (POC co-financing)
- Clusters for development of new technology
- Support of public sector (also through funding programmes and R&D)
- patent/trademark simplification (long and complicated registration process)

- access to knowledge (facilitate university R&D to be supported by private sector)
- public infrastructure (public clouds, cybersecurity services…)

An alternative way to help fintechs, different than lowering security requirements, is letting them use the infrastructure from the incumbents. This should be done at a price that acts as an incentive to keep on investing in it. There are precedents when government infrastructures have been opened to other players, such as in the case of railings: this has always been done under payment. The same logic should apply if banking infrastructures are opened to third parties.

However, the digital speed does not provide the market with years to wait for a revision. The digital principle of "fail fast, learn fast" should be rendered applicable. In a changing world, it is necessary to make sure that decisions are reversible and that authorities can apply different measures to adjust for change.

The banking sector cannot bear all the costs of financial innovation. So it is necessary to find an alternative way to support the Fintech startup ecosystem, without creating an irreversible unlevel playing field. This should start by establishing a regulatory framework in which all market participants are required to follow the same rules. (We cannot make concessions on consumer protection, on market integrity, on safety nor on cybersecurity. Rules have to follow high standards and should be the same for all). It is important that authorities leverage the deployment of new solutions with technological neutrality, proportionality and integrity principles, in order to contribute to a level playing field among all players.

FinTech has reduced barriers to entry in financial services markets

3.3 What are the existing regulatory barriers that prevent FinTech firms from scaling up and providing services across Europe? What licensing requirements, if any, are subject to divergence across Member States and what are the consequences? Please provide the details.

In our view, the main barriers faced by Fintech new entrants to scale up and provide services crossborder are not so much related to regulation as to its size and initial capital investment. In terms of licensing requirements, new entrants and incumbents face the same challenges: despite the use of passporting, there are usually local requirements to be fulfilled before offering services in a new country. Those should be streamlined for all players to allow for a more vibrant ecosystem.

Practical difficulties to cross-border operations are sometimes extremely subtle, as in the requirement of certain member states (e.g. Germany) for financial services providers operating under passporting to use local IBAN numbers for accounthoders, which is impossible to achieve by a company established in a different member country. The enforcement of the European passport should be guaranteed. Therefore, the IBAN from any

European Country should not be discriminated in any EU country, or else obtaining national IBANs should be automatic.

As we already mentioned along our response, we believe that FinTech regulation should ensure a level playing field for companies engaging in similar activities, with similar risks, in any European country. Today, two main barriers to this vision are the lack of regulatory homogeneity across countries and the lack of European regulations for certain activities.

Currently, we witness how certain European countries are developing national regulations or supervisory practices that create inequalities within the European Union. As an example, the UK and the Netherlands have launched regulatory sandboxes that make it easier for innovators to develop FinTech innovations in those jurisdictions.

3.4 Should the EU introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market? If the EU should introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market, please specify in which specific areas you think this should happen and what role the ESAs should play in this. For instance, should the ESAs play a role in pan-EU registration and supervision of FinTech firms?

Yes. Any provider of financial services must have a license that ensures the services are being provided with certain characteristics and level of quality. Also, different types of licenses should be put in place, asking for different security obligations (data protection, transparency level, reporting), or capital requirements, depending on the services provided.

We support FinTech licenses for specific activities **including passporting**, to facilitate the quick development for Fintechs across Europe would be positive as they would ensure a balanced framework and security in areas that are unregulated (digital assets, crowdfunding…), or that are currently using licenses that are not really adjusted to their activities (cash on ledger regulated as electronic money). This way, effective supervisions of the risks can be ensured. We support the fast passporting of such licences, as it will also help to reduce costs and inefficiencies.

However, we do not believe that generic licenses should be put in place: each activity entails specific risks, so there should be a specific licensing process performed by specialized authorities and further controlled by them

What is crucial is that players are subject to the same regulation because of the products or services they offer, and not because of their nature or size. European rules should focus on how to best manage stability, integrity and consumer protection risks while encouraging innovation and healthy competition.

3.5 Do you consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial

services within the Single Market? If so, please explain in which areas and how should the Commission intervene.

Yes. Technological innovation in financial services should be encouraged and have a neutral regulatory treatment regardless of the type of entity that undertakes it. Being a bank shouldn't penalize the activities. The banking regulatory framework should not affect digitalization.

Besides, proportionality in financial services should be linked to individual risks, not to the size of firms. Otherwise, smaller players would be better suited for disruption, creating less chances for incumbents to transform themselves, thus creating greater financial instability. Consequently, European regulations should focus on how to best manage stability, integrity and consumer protection risks, rather than just promoting greater competition at all cost.

A particular case can be found in cybersecurity. The ICT Risk Assessments should be proportional and based on principles and international recognized standards such as ISO and NIST. Moreover, this proportionally should give room to the risk appetite of each company, based on proven evidence that the risk has been mitigated or controlled.

3.6 Are there issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market? Please elaborate on your reply to whether there are issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market, and explain to what extent regulations on data localisation or restrictions on data movement constitute an obstacle to cross-border financial transactions.

Yes. The ability to transfer data both within and out of the EU is vital for the banks' activity, no matter their size or their geographic location. To achieve cross-border data flows, there must not be restrictions on data localisation, otherwise the competitiveness and growth of EU companies and the efficiency of its operating functioning can be threatened.

For instance, we observe that one of the hindrances to a consistent European Union (EU) and Global regulatory framework for Cloud Computing in Financial Services is related to regulation and domestic laws which establish barriers to the geographic location of the physical Cloud Computing infrastructure.

3.7 Are the three principles of technological neutrality, proportionality and integrity appropriate to guide the regulatory approach to the FinTech activities? Please elaborate on your reply to whether the three principles of technological neutrality, proportionality and integrity are or not appropriate to guide the regulatory approach to the FinTech activities.

Yes. We fully agree with them.

Technological neutrality (understood as same activity, same regulation) is necessary but not sufficient to guarantee a level playing field. Equally important is to have same supervision (to equal risks to those inherent to the banking activity). Moreover,

proportionality is needed, as a risk-based approach that takes into account specific activity risks, and not whole company risks by default. However, there are cases where proportionality cannot be applied: in case of cybersecurity and consumer protection all players should make sure that they comply with the highest standards. Small new entrants should be supported through other means than an unlevelled regulatory framework.

It is our understanding that a technology-agnostic principle should also be included, as it facilitates the self-selection of the best technologies by market forces. This can be practically applied by adopting international recognized standards that are also agnostic to technology. In these cases, some type of guidance is required to avoid "reinventing the wheel", which could potentially end up with many different standards and fragmentation.

Role of supervisors: enabling innovation

3.8 How can the Commission or the European Supervisory Authorities best coordinate, complement or combine the various practices and initiatives taken by national authorities in support of FinTech (e.g. innovation hubs, accelerators or sandboxes) and make the EU as a whole a hub for FinTech innovation? Would there be merits in pooling expertise in the ESAs? Please elaborate on your reply to whether there would be merits in pooling expertise in the European Supervisory Authorities.

A European framework is needed to foster innovation at EU level while also avoiding regulatory arbitrage and competition among the different national initiatives. Given that at this point there are already a number of national initiatives that could create distortions at the internal market, it would be welcome that EU authorities establish basic principles for harmonization through the adoption of guidelines or recommendations and the identification of good practices.

The objective would be the establishment of pan-European initiatives, such as a European sandbox framework. The level of integration on this matter could follow the approach of the European Banking Union.

We share the view that it would be convenient to have experts at the ESAs and National Competent Authorities that could monitor the innovation advances, with a broad perspective. In this regard, it is of interest to establish a coordinating authority to unify these efforts, as well as it would ease the establishment of agreements with external innovation ecosystems, which might benefit all EU stakeholders, as further links with new markets might aid the EU in its global leadership goal.

3.9 Should the Commission set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns? If so, please specify how these programs should be organised.

Yes, it is a good idea to convey and share knowledge among the different market participants, experts, and regulators and supervisors. With these kind of programs, it is not only possible to get to understand how certain new technologies, such as DLT, work, but

also to know in more depth the possible implications of the new technologies in areas as relevant as data protection or cyber-risks, which are common to all financial innovations.

An innovation Academy could help to centralise all the efforts related to the development of a FinTech friendly environment in a coordinated way. One of the key assets would be the creation of learning mechanisms to ensure that all knowledge created could be used for the interest of all stakeholders. In this sense, one of the main objectives of the introduction of an Innovation Academy could be the establishment of learning mechanisms providing guidance for future projects, such as the rationale behind the approval or denying of certain financial innovation projects and best practice case studies, as well as reports regarding the use of new technologies and forecasting studies.

Another important issue is ensuring that all stakeholders are represented (industry, consumer representatives, academic researchers and authorities). Certain projects could impact legal requirements from more than one authority. To ensure that there is a correct dialogue between all legal jurisdictions, representatives from all of them should take part of this Innovation Academy.

The approach could be inspired by the private model of accelerators or incubators, in research consortiums or already existing innovation hubs. Furthermore, all examples can come from the financial sector or from other knowledge areas.

3.10 Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS? Please elaborate on your reply.

Yes. As we answered in question 3.8, some high guiding-principles for harmonization should be established. All sandboxes should be harmonized in terms of connectivity and technology to apply and also in terms of the legal framework to avoid regulatory arbitrage and competition among the different national initiatives. This harmonisation should be inclusive and take into account all interest parties regardless of their size of business model.

It is of interest to note that this legal framework should include how these sandboxes must operate: entry requirements, what happens while in the sandbox and how the project should enter the market. Furthermore, as this is a learning process, a review of the final decision should be publicly shared for all interest parties to understand the rationale of this outcome. Nevertheless, a list of potential regulations that might be softened, tools that all participants might access and the limitations related to customer protection and systemic stability must be listed prior entering the sandbox.

Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border? If so, who should run the sandbox and what should be its main objective?

Yes. It would be very useful to test some innovations that are being developed cross-border, as current DLT projects.

The creation of a special regulatory sandbox for all types of FinTechs (including banks) willing to operate on an intra-European, cross-border basis is positive. However, as stated in question 3.8, it is also of interest the establishment of links with other innovation ecosystems outside the EU and, in this case, with regulatory sandboxes from other jurisdictions.

3.11 What other measures could the Commission consider to support innovative firms or their supervisors that are not mentioned above?

Those related to digital knowledge, targeted to individuals and companies could be further explored as well as fostering to advance towards a cashless society.

In relation to the DLT projects that are currently being developed by many private consortia, it would be very useful to have legal experts within authorities in order to be able to advance in the interesting use cases under development.

Furthermore, due to the growing complexity of the ecosystem, authorities must strengthen their supervisory role on the new services that arise, taking a proactive role when the service provider does not meet legal requirements or exceeds its license, providing services that they have not been authorised to. This measure ensures that customers only access safe and secure financial services and avoids misuses that might damage the reputation of all services providers.

Role of industry: standards and interoperability

3.12 Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision?

No. However, we believe that the development of standards should be left to the market forces according to the needs and convenience and ready for evolution when technology changes.

Having said that, although we do not expect authorities should set the standards nor impose very prescriptive regulations, it would be helpful they promote some framework or space where the different players can meet and reach agreements to define jointly the standards as well as the draft of some certain lines, as in the case of PSD2's RTS.

Moreover, from the point of view of Security, the recommendation by supervisors of standards to follow, such as NIST, ISO 2700X or COBIT would ease compliance. Sometimes these guidelines or standards should be clearer to avoid disputes.

Finally, authorities should focus on solving overlaps between different regulations or supervisory rules such as those of NIS Directive, National Critical Infrastructure laws and ECB ICT Risk Assessment as well as on ensuring that non-bak Fintechs are subject to explicit cybersecurity and outsourcing requirements. This will foster market efficiency and fair competition.

Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities?

We do not believe that the current level of data standardisation and interoperability is an obstacle for the use of outsourcing opportunities (See question above). Indeed, as non-bank FinTech operations are not always subject to oversight by financial authorities, these companies are better positioned for outsourcing than incumbent financial institutions.

3.13 In which areas could EU or global level standards facilitate the efficiency and interoperability of FinTech solutions? What would be the most effective and competition friendly approach to develop these standards?

In our view the objectives of efficiency and interoperability can only be enabled by standards if they are developed at a global level, are outcomes based, technology agnostic, transparent, and inclusive, and are promoted by the market forces.

EU institutions and market players should have an active voice in global standardization organizations such as ISO and avoid that other countries try to impose a specific standard or obstruct their development for political or economic purposes. Therefore, we welcome the adoption of any measures aimed at supporting EU engagement with these organisations.

3.14 Should the EU institutions promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses? Please elaborate on your reply to whether the EU institutions should promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses, and explain what other specific measures should be taken at EU level.

No. Technology services providers should develop open source solutions where they are needed, but this should not be imposed by EU institutions. In our view, authorities may have an important role in the promotion of frameworks where the private sector can collaborate and debate about it.

Challenges. Securing financial stability

3.15 How big is the impact of FinTech on the safety and soundness of incumbent firms? What are the efficiencies that FinTech solutions could bring to incumbents? Please explain.

In our view, FinTech solutions – in a B2B collaborative model - bring to incumbents efficiencies especially in retail and commercial banking, and in three specific fields:

1) Being able to meet customer demands:

The entrance of new digital providers, and the proliferation of intermediation services that increase transparency and comparability, is increasing competition in the financial services

industry. This adds additional pressure to the banks' profitability and forces banks to transform themselves in order to gain efficiency and offer new value propositions to customers. To that end, the regulatory and supervisory framework must allow banks to be agile in adopting new technologies and developing innovative products and services.

2) Rationalization of banking processes

3) Costs – savings:

All digital technologies bring significant efficiency gains for the financial system, both at the front and back end, as has been explained in the previous sections of this consultation. Efficiency gains arise from the application of technologies that automate or disintermediate processes and from the use of a more flexible and scalable IT infrastructure. The regulatory and supervisory framework should facilitate the adoption of these technologies while keeping risks under control.

Moreover, the application of digital technologies may have positive impacts for the soundness of the financial system. For instance, the so called "RegTech" solutions improve risk management functions, and cloud computing may reduce traditional IT risks, such as capacity or resilience.

4. Balancing greater data sharing and transparency with data security and protection needs

4.1 How important is the free flow of data for the development of a Digital Single Market in financial services? Should service users (i.e. consumers and businesses generating the data) be entitled to fair compensation when their data is processed by service providers for commercial purposes that go beyond their direct relationship?

We believe that data is one of the most valuable assets of institutions in the digital world. Allowing European companies to extract the highest value from their data will positively impact on their competitiveness.

Therefore, any regulatory development in the field of data should guarantee that players be allowed to extract value from the work they perform with data, while preserving data protection and privacy rights for consumers.

The importance of having an appropriate competitive environment with a level playing field for all the different players should be the main reason for ensuring that not only banks have to comply with high standards in order to use personal data. This level playing field needs to be achieved both within the EU between different types of firms, e.g. banks and non-banks; and between EU and non-EU firms.

Additionally, it is worth to mention that, given its strategic value, data issues are a key commercial and strategic business decision for a company. There are some players that invest huge quantities of resources in order to ensure that their data are of good quality, so they should have the possibility to exchange them for a price that is convenient for both sides: the market should adjust this.

Customers are already being compensated through the access to digital services that are being proven very convenient for them. The benefits that individuals obtain come from the access to more tailored and personalised services, which fit better their preferences and needs. Hence, enough transparency should be given to the customers when they provide their data.

When the service users' data is processed by service providers for commercial purposes that go beyond their direct relationship, the users generating the data should have the opportunity to achieve an incentive or benefit. However, we should not understand the fair compensation as a payment to the user or as a direct economic compensation for allowing data processing. The benefit is derived from the user having access to a more personalised, global and tailor-made service or having certain service/products benefits in exchange.

Nevertheless, we should also take into account the different kind of data, bearing in mind that enhanced data are part of any organization know-how, which means that they should be the ones achieving the benefit from it, as they have invested resources and intelligence in order to enhance raw data.

It is positive that the system is provided a framework that allows sharing the data but it is also necessary that incentives to maintain high quality data still exist, so players should be free to establish the price. There is already a lot of transparency in data gathered by banks but still not so much in other relevant data, such as those of merchants, delivery, etc.

Storing and sharing financial information through a reliable tool

4.2. To what extent could DLT solutions provide a reliable tool for financial information storing and sharing? Are there alternative technological solutions?

One of the main characteristics of DLT is its immutability. The use of sequential hashing and cryptography, combined with the decentralized structure, make it virtually impossible for any party to unilaterally alter data on the ledger. This can be used by organizations handling sensitive information to maintain the integrity of data, and to prevent and detect any form of tampering. In this sense, there are many financial processes and services that could benefit from the immutable nature of DLT storage: Customer data, contract information, property rights, and in general "digital fingerprints" of any kind of agreement are some of the types of information that could be stored in a DL.

The alternative to DLT solutions are traditional databases operated by central authorities (CCP's, regulators, FMI's, etc.).

4.3 Are digital identity frameworks sufficiently developed to be used with DLT or other technological solutions in financial services?

No. We believe that the digital identity framework still needs to improve in the following aspects to be used with DLT: interoperability, standards, authentication, key management, etc. Further public support is needed to develop more advance solutions.

4.4 What are the challenges for using DLT with regard to personal data protection and how could they be overcome?

In our view, and in the line with the Commission's objective of being technology neutral, DLT should be treated the same way as any other technology in regard to personal data protection: Personal data should only be shared with parties that have explicit permission to have access to the data, regardless of encryption. Indeed, encryption is a security measure and it is not a tool that implies anonymization. However, strong encryption is a measure that should be considered and promoted.

DLT implies high quality data, being consistent, complete and accurate. However, while DLT is global, data protection regulation is fragmented and as for the use of Blockchain as a tamper proof source of truth in relation to the information stored on it, regulatory fragmentation implies a challenge.

In that sense, the challenges of DLT in regard to personal data protection are similar to those identified along this response, as for instance the issues related to geographic location (transfer of data across boundaries).

Perhaps one of the biggest challenges in regard to personal data protection that this technology faces comes from how the right to erasure or to be forgotten (introduced by the GDPR) can be compatible with the immutability of the DLT.

Blockchain does not necessarily threaten data protection but it can also be a privacy enhancing technology. It is a matter of applying the privacy by design principle and privacy impact assessments whenever designing a blockchain technology based service or product.

The power of big data to lower information barriers for SMEs and other users

4.5 How can information systems and technology-based solutions improve the risk profiling of SMEs (including start-up and scale-up companies) and other users?

New technology-based solutions and information systems have increased the amount of information available on SMEs, via higher interconnections (i.e connecting to official tax databases) or through the use of new channels, as for instance online platforms and social media, that can be used to enrich the banks' credit scoring.

This increases the possibility for banks to serve customers that couldn't reach traditional banking finance, such as young companies without credit history but for which predictions can be made based in their behavior related to other aspects. It is critical that regulators and supervisors allow banks to test these solutions, starting at low scale, and be able to extend them if they succeed.

4.6 How can counterparties that hold credit and financial data on SMEs and other users be incentivised to share information with alternative funding providers? What kind of policy action could enable this interaction? What are the risks, if any, for SMEs?

There should be a framework that supports a truly free flow of non-personal data, such as credit and financial data. **Truly free means that no player should be forced to deliver these data**, Incentives should be kept to ensure that high quality data are gathered and maintained. For this, it is essential that each player has the possibility to extract value from the data they manage and decide whether to share them and under which conditions.

In terms of policy action, much has already been done in the financial sector through rules such as PSD2 (that allows account information service providers to access the transactional data in a very convenient manner) and more generally in GDPR, which recognizes the citizens' right to port their personal data in the most efficient manner.

The market is already very open and does not require any additional provision until these regulations are fully in place and an assessment is being made that more has to be done. Especially, given that the financial sector has been one of those more affected by initiatives

to open data, in relation to the rest of sectors that do not have similar measures (and whose data is also relevant for the provision of credit).

Additionally, certain measures could also be of help to increase funding for SMEs, such as allowing banks to enter crowdfunding platforms or partner with Fintech SMEs for this purpose without being applied the full consolidated banking framework.

The sharing of information could also be facilitated through the adoption of shared standards enabling a faster and more effective relevant data flow between firms, i.e. for risk assessment.

On the other hand, data protection and cybersecurity should be kept in mind so the information sharing does not put in danger the efforts of the industry to maintain high safety standards.

Security

4.7 What additional (minimum) cybersecurity requirements for financial service providers and market infrastructures should be included as a complement to the existing requirements (if any)? What kind of proportionality should apply to this regime?

The gap between technology and regulation is particularly important in cyber security, as a result of new solutions which are evolving at a faster pace than regulatory frameworks. In this regard, no new requirements should be established until there is a clear picture of the impact of regulations on cybersecurity being implemented currently. We believe that regulatory efforts should focus on the simplification of the current regulatory framework

The number of cyber-attacks happened in recent years is a proof that no company is completely safe. And the biggest problem, in addition to the theft of personal and financial data, is the impact they could have on systems, interrupting the normal activity and mining the customer confidence.

Cybersecurity requirements should be proportional to take into account the complexity of the company, but for smaller companies they should not be lowered in order to ensure an adequate level of protection. The system is as safe as the lowest point of its security chain. Once the framework has been opened by regulatory initiatives such as PSD2, all participants should bear the responsibility to keep it safe. If needed, the authorities could envisage establishing cyber security infrastructures to support compliance for the smaller entities.

4.8 What regulatory barriers or other possible hurdles of different nature impede or prevent cyber threat information sharing among financial services providers and with public authorities? How can they be addressed?

In our opinion, the following act as hurdles that impede information sharing on cyber threats and should be addressed by EU and national competent authorities:

Regarding reporting:

- The need to report incidents to the relevant competent authorites translates into requirements on providers to report the same type of incidents to different regulators, which creates a burden for all companies regardless of their size. It is necessary not only to harmonize these requirements but to establish a one-stop-shop mechanism for incident reporting to distribute to all relevant authorities and regulators in relation to different legislative pieces. Reporting procedures, templates and methodologies used in the different Member States should be streamlined and made consistent.
- Major incidents reported should be anonymised and shared back with private sector; this would provide them with interesting data on the incident itself and the modus operandi and, in turn, allow them to prevent future such incidents and to have better and shorter intervention when an incident occurs.

Regarding information sharing among private companies and with public authorities:

- Information on incidents should be reported not only to supervisors and regulators, but it would add value to the market if this information was also shared between companies on a confidential basis. In particular, sharing information or distribute early warnings on major incidents between entities would increase information intelligence in other financial institutions and allow them to take pro-active measures to avoid or prevent those or similar incidents. FS-ISAC in the US and CiSP in the UK are examples of information sharing among public and private companies, but a similar initiative should be set up at EU level, led by ENISA together with the ECB and EUROPOL.

- It would be necessary to allow and define at EU level data sharing among private companies for cybersecurity purposes, including harmonizing the pieces of data that can be shared. National Data Protection rules represent a barrier to share certain pieces of data among private companies. For example: the IP address of the attacker has to be reported to the national competent authority in Spain but cannot be shared with other private companies for cybersecurity purposes because it is considered personal data. Moreover, in case users are denied access to a given service on the basis of information stemming from preventive measures of other service providers and this information was erroneously interpreted, it could be considered an anti-competitive and/or discriminatory act

What is really necessary is to promote stronger public-private cooperation in cyber security.

4.9 What cybersecurity penetration and resilience testing in financial services should be implemented? What is the case for coordination at EU level? What specific elements should be addressed (e.g. common minimum requirements, tests, testing scenarios, mutual recognition among regulators across jurisdictions of resilience testing)?

There are already in place a number of cybersecurity penetration and resilience testing in financial services.

Regarding financial market infrastructures, CPMI together with IOSCO released in June 2016 their Guidance on cyber resilience for financial market infrastructures. They advocate the safe resumption of critical operations within two hours of a disruption. We consider that this 2-hour period is not technically feasible in case of a serious cyberincident and this Guidance should be revisited. Besides, financial markets infrastructures are concentrating transactions from different markets and currently it is not clear how priorities would be set in case of failure and how to model and test different existing possibilities for recovery.

We believe that the authorities could use as reference the UK CBEST Vulnerability Testing Framework developed by the Bank of England, as it enables banks to think in the future cybersecurity challenges instead of adjusting their systems to cybersecurity supervisory requirements that are based on information from the past.

Regarding the future update of the NIS Directive, it should contemplate also the other players in the industry such as non-bank FinTech companies, hardware and software manufactures as well as SMEs.

Finally, free awareness and training campaigns for those companies that are identified -under some type of prioritization scheme- as the weakest link in the chain would be useful.

At EU level it would be necessary to map critical economic functions and understand which are the single points of failure and the available alternatives in case of cyberattack.

4.10.1: What other applications of new technologies to financial services, beyond those above mentioned, can improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing?

As stated in answer 3.7, there is a principle of technology-agnosticism that should be included. Innovations are uncertain by nature, therefore we must assume that new technologies will arise which are not analysed in this consultation. In this regard, we consider of special interest that regulators focus on the effects of the application rather than in the technology itself in order to avoid the creation of barriers for future developments currently unknown.

4.10.2: Are there any regulatory requirements impeding other applications of new technologies to financial services to improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing?

The new Payment Services Directive (PSD2) will grant individual and business clients the right to directly transfer their bank account data to third-party payment service providers (TPPs) in a standardized way. At the same time, the General Data Protection Regulation (GDPR) will introduce a new right for data subjects to port the personal data provided to any firm they are engaged with. To achieve a level playing field in the access to clients' data under PSD2 and GDPR, it is essential that the right to personal data portability is implemented in a way that is consistent with PSD2.