15 June 2017

EBF_026943

EUROPEAN BANKING FEDERATION (EBF)'S RESPONSE TO THE EUROPEAN COMMISSION'S CONSULTATION ON FINTECH: A MORE COMPETITIVE AND INNOVATIVE EUROPEAN FINANCIAL SECTOR

KEY MESSAGES

The EBF welcomes the European Commission's consultation and the creation of its FinTech taskforce. The taskforce serves not only as a bridge between policy makers and the industry but also as an essential horizontal connection between policy makers in financial regulation and the digital agenda in the EU.

Responding to the EU consultation on financial technology, also known as FinTech, the European Banking Federation is submitting a response which underlines its desire to see the creation of a customer-centric and inclusive ecosystem in which all actors, ranging from small start-ups to established multinational banks, are committed to serving clients with innovative financial services.

- **Promote the right definition of FinTech:**

  FinTech refers to "financial" and "technology" meaning the application of new technologies to financial services. It is however sometimes understood as referring only to start-ups or tech-giants that develop innovative financial services solutions. Innovative financial technology based solutions and services are increasingly being developed by banks. This is why it is important to point out that the "FinTech" concept should be understood as finance enabled by or provided via new technologies, affecting the whole financial sector in all its aspects. Whereas the value chain increasingly includes alternative actors such as start-ups or tech giants, any actor can be a FinTech, regardless of the kind of legal entity it is. The FinTech concept should be connected to the products and services offered to the client and is therefore activity/services based.

- **Put consumers' interests first**

  Consumers around the world are quickly becoming digital. They want to manage their money more proactively, to simplify and streamline the management of their financial portfolio, and be able to derive tangible benefits from their service providers. As a result, consumers expect a new kind of service proposition from banks, fitting to the digital age.

  In response, banks - and other providers - are assessing, developing and using innovative and technological capabilities (such as open APIs, blockchain, robo-advice and machine learning) to develop new delivery channels as well as to enhance services and products that deepen the relationship with their customers.
  In this fast changing environment, consumer protection should remain the key priority. A level playing field has the role of ensuring consumers are not put at risk and that financial stability is maintained, irrespective of the service provider. Development in the field of FinTech could lead to a series of changes to financial services with new players, new solutions and new products / services. However, any changes must not undermine consumers' data security nor their confidence in the European financial sector.

- **Equal contribution to an innovative and competitive ecosystem: "same services, same risks, same rules and same supervision".**

  The Digital Single Market is an opportunity for all operators willing to embrace the digital transformation: authorities, FinTech (banks, non-banking FinTech/FinTech start-ups) corporates and consumers. The same regulatory conditions and supervision should apply to all actors (large digital players, financial institutions and start-ups) who seek to innovate and compete in the FinTech system. Any regulatory framework must keep barriers to entry to a minimum, and should also not hinder incumbents' ability to innovate and develop. As mentioned previously, the Commission must always apply the principle of "same services/activities, same risks, same rules and same supervision" in order to ensure consumer protection and market integrity. Regulation should be also neutral regarding technological developments and business models. For competition and a Digital Single Market for financial services to succeed, improvements are needed in current legislation, and regulatory requirements must be proportionate to ensure the current framework does not hamper innovation and competitiveness. Furthermore, it is indispensable that players across the board contribute to the appropriate level of investment in infrastructure. Market incumbents must preserve a level playing field allowing some degree of connectivity to newcomers, however it is important to ensure that all market participants contribute to the appropriate level of investment in infrastructure.

- **Banks' partners and competitors in their digital transformation - we are all innovators**

  We are likely to see increasing cooperation and partnership among banks and new FinTech start-ups providing innovative products and services to the market. Indeed, the arrival of FinTech start-ups and the establishment of digital platforms has spurred innovation, accelerated the transformation of banks and opened a door to new win-win collaborations. While there are still good reasons for banks to rely on internal IT departments, there is considerable potential to create value — for themselves and the economy at large — by nurturing an ecosystem of start-ups and technology innovators that can assist banks in developing shared platforms thereby increasing resilience and cost effectiveness of banking and payment systems. Banks have a lot to offer to FinTech start-ups, in particular, specific financial expertise (risk assessment, evaluation and management), scalability owing to their large customer base, as well as many years of experience in providing clients with operational security in a highly regulated sector, not to speak of financing needs. The respective strengths of both banks and FinTech start-ups mean that both will often do better by cooperating rather than by competing.

N°	Questions	EBF Answers
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?	FinTech refers to "financial" and "technology" meaning the application of new technologies to financial services. It is however sometimes understood as referring only to start-ups or tech-giants that develop innovative financial services solutions. Innovative financial technology based solutions and services are increasingly being developed by banks. This is why it is important to point out that "FinTech" concept should be understood as finance enabled by or provided via new technologies, affecting the whole financial sector in all its components. Whereas the value chain increasingly includes alternative actors such as start-ups or tech giants, any actor can be a FinTech, regardless of the kind of legal entity it is. FinTech concept should be connected to the products and services offered to the client and is therefore activity/services based. The involvement of banks in FinTech comes with huge investments, jobs and growth, for all sorts of suppliers (including incumbent tech giants). While there are still strategic reasons for banks to rely on internal IT departments, there is considerable potential to create value — for themselves and the economy at large — by nurturing an ecosystem of start-ups and technology innovators that can assist banks in developing shared platforms increasing resilience and cost effectiveness of banking services and payment systems. In practice, many banks have their own incubator programme, where an issue / challenge is set, then the bank enter into a process of reasonable length to understand FinTech start-ups' propositions and work with them to develop their company, product and services so to get them into a robust position to sell within the regulated sector. Another option is the use of venture capital to acquire these new companies and merge them with the current product mix of the purchasing bank. A high percentage of banks views the possibility of partnerships with non-banking FinTech/FinTech start-up with great interest, with the objective to obtaining concrete benefits that enhance specific key business areas, products and/or services by leveraging:

		a) solutions focused on cost reduction via improvement to processes or replacement of IT platforms/ IT solutions with new business models or new technologies; b) solutions enabling banks to attract and on-board new customers, to improve the relationship with customers or to increase the offer of new and innovative products/services; c) risk management; d) cybersecurity (e.g. fraud prevention and data protection); e) regulatory technology (RegTech); f) processing solutions in the payments or securities space; allowing the testing of new technologies such as Distributed ledgers, Application Programming Interface (API); g) Artificial Intelligence (AI) applied to Robotic Process Automation (RPA) (advisory/ for advisory), or applied to Regulatory Technology (Regtech); h) Corporate and Investment Banking, SME banking solutions, IT core banking solutions, and solutions focused on enhancement of data quality and the data architecture. Also, any FinTech solution that could optimise administrative processes for business such as reconciliation, forecasting, B2B procurement workflows, strategic advisory, fraud prevention, or alternative ways of funding should be welcomed. Banks also have a lot to offer to FinTech start-ups, in particular, specific financial expertise (risk assessment, evaluation and management), scalability owing to their large customer base, as well as many years of experience in providing clients with regulatory-driven high levels of operational security. One of the challenges is that smaller companies are often less prepared to meet all the regulatory requirements to which banks need to adhere, and there is often support from banks' compliance areas to bridge the knowledge gap. Although some degree of competition, the complementary strengths and weaknesses of all FinTechs (banks, non-banking FinTech/ FinTech start-ups) mean that those entities will often do better by cooperating rather than by competing. The Commission must always apply the principle of "same services, same activities, same risks, same rules and same supervision" in order to ensure consumer protection and market integrity. It is however important to keep in mind that the collaboration of banks and non-banking FinTech/FinTech start-ups for the deployment of FinTech solutions is constrained by certain regulations (e.g coexistence of 'profiling' with the right to erasure (`right to be

		forgotten') within the General Data Protection Regulation (GDPR) might be an issue for the use of Distributed Ledger Technologies). In addition, most solutions provided by technology companies large and small are developed on a cloud first basis. Removing barriers to the use of cloud computing in financial services (discussed below) is key to increasing the rate and degree of collaboration between banks and start-ups in the area of FinTech.
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.)? **(Yes/No/Don't Know- not relevant)** **<u>If Yes,</u>** if there is evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services, at what pace does this happen? And are these services better adapted to user needs? Please explain.	**YES** Certain forms of automation in financial advice are already widely adopted and commonly accepted (e.g. providing online investment advice when a client purchases financial instruments online, having a customer completing a MiFID questionnaire online, having a customer providing information needed to apply for a mortgage credit online etc.). Robo-advice typically combines a range of financial tools to, among other things, manage clients' 'investment portfolio and optimize it, based on the client's investment goals and risk appetite. Banks have substantial experience providing detailed personalised financial planning services to the benefit of the customers (it also includes threat analytics including cyber security, improved AML and KYC functions, more holistic understanding of the customer resulting in improved offerings etc). The automation of financial advice would be another step in this direction. As banks have invested great resources into improving the product offering it has become clear that, automated financial advice could result in significant consumer benefits: ▪ **By enabling greater financial inclusion and simplifying the investment process for mass market:** It is expected that robo-advice main contribution will be bringing portfolio investment to client groups who previously had no access to it, in decreasing the price (because of IT developing, maintaining and security costs, the cost reduction will also depend of the development of specialized teams). The ubiquity/ geographic scope of financial advice availability will also improve. ▪ **By enhancing customer experience:** The continually evolving data-driven approach can be applied to and improve many processes that might typically rely on intuition or limited or incomplete information. In compliance with data protection regulation and

		data usage requirements, robo-advice will bring a wide range of choices in terms of services offered and customization capabilities driven by, better use of this data through advanced analytics e.g. through: - offering contextualised, targeted products and experiences; - making more accurate credit-worthiness assessments; - providing better financial advice; - reducing costs for consumers; and - better protecting customers from fraud. Financial institutions of all types, whether incumbent, challenger or digital only, are investing great resources to deploy such service within the framework of the relevant regulation which already governs financial advice and the use of personal data (MiFID and GDPR being the most relevant). However, in many European countries, automated financial advice is still in its infancy as well as the collaboration with non-banking FinTech/FinTech start-ups. It is therefore too early to have evidence that automated financial advice solutions will in fact increase the customer base. The pace of adoption will, naturally, depend on the degree of maturity of each market, (broadband and Wi-Fi infrastructure etc.) and the behaviour and requirements of customers. It remains to be seen if and when they will ever be used and accepted on a large scale (e.g. fully automated asset management or robo-advice) and if this would even be possible regarding stringent data protection and security rules. Banks and other financial institutions have indeed long been custodians and users of data, and have well established systems and protocols for using and protecting sensitive data on a large scale in compliance with the applicable legal and regulatory requirements. Financial services use cases requiring implementation of the highest levels of confidentiality for data handling / storage mechanisms. Often solutions that are well established in other industries – for example cloud storage – are difficult to implement in practice in financial services'. It has to be noted that appropriate technical and organisational safeguards are unavoidable in this context. Especially when cloud storage is outsourced, confidentiality has to be of great concern.

		Where, EU legislation often departs from the idea of a physical meeting and the provision of physical documents, here is a need to adapt legislation to a fast growing digital development. Finally it is important to note that automated financial advice currently focuses more on the provision of information, comparison websites and calculators. A clear distinction should be made between the use of an automated tool and the use of automated financial advice, and consequently also between MiFID and non-MiFID services (investment services should be regulated under MiFID but not the other types of services like comparison websites). There is no clear line between an automated tool and automated financial advice. In fact a grey zone area has developed. Sites, often run by start ups, which seem to provide only comparisons and guidance, in reality provide consumers with advice. Further clarity in this regard should be provided notably on what is subject to MIFID and what is not. We would like to stress that increased automation will not remove the possibility of a personal contact for clients with a financial adviser. Banks will continue to cater for both the digital savvy and its traditional client demographics. Financial needs will still require access to human advisers to assess best approaches to financial structuring. In many cases, an IT tool is used to recommend the investment advice previously provided by an asset manager or the research department of an investment firm. Consumers have different needs and preferences, while some will want to continue having face-to-face meetings, others prefer digital tools. These tools can indeed be used either to provide full robo-advice or to improve the internal procedures to provide traditional in-presence financial advice. The difference is only the channel used to interact with the customer.
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?	**NO** It must be remembered that Artificial Intelligence (AI) is still in its initial growth phase and the technology continues to develop and evolve. The use cases of AI are manifold as AI based software will push the limits of automation. Artificial Intelligence is an umbrella term to cover a confluence of multiple technologies, such as machine learning, which includes deep learning, cognitive computing, natural language processing, neural networks, etc.

	(Yes/No/Don't Know- not relevant) 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.	Regulators must be prudent when taking steps in this context. In our view, it is important, first to understand how this technology works and subsequently the potential impact on the consumers before taking any new regulatory measure. The ethical, legal and societal impacts are also factors to be considered. But it is also paramount to ensure that the regulatory environment fits for the use of AI by promoting innovation and legal certainty. Premature legislative action on this front could also potentially result in a limit to the consumer and market benefits that the technology might bring. It could result in proposing a regulatory solution without knowing what kind of opportunities AI could really provide or what kind of problems AI could solve. It would then prevent this technology from delivering its promises of a less expensive, more calibrated and more inclusive access to investment advice and from contributing to the objectives of the Capital Markets Union (CMU) and the Digital Single Market (DSM). It should also be kept in mind that AI is not solely a financial services' issue. On the contrary, a cross-sectoral and technology neutral approach should be considered, regardless of the legal entity of the company. In our views, there are already a number of regulations in existence which impact upon the working of AI and which must be considered. The use of personal data already has regulatory oversight in a number of areas, for instance antitrust for pricing. Under the General Data Protection Regulation (GDPR) there is already transparency requirements imposed on data controllers around automated processing. Banks on their side are already heavily supervised and have to comply with many legislative requirements so an additional supervision, focusing only on algorithms would not be appropriate, but considered disproportionate. A level playing field is paramount, it must ensure consumer protection, privacy, security, liability and competition as well as empower Supervisory Authorities to request information, carry out on-site inspections and issue binding provisions and sanctions. Financial activity must be performed under equivalent supervision requirements (e.g. there are further requirements under Markets in Financial Instruments Directive 2 (MiFID 2) that must be considered in order to ensure regulatory alignment).

		No enhanced oversight on AI should apply, as it could be detrimental for the development of this technology but rather a dialogue with regulators should be encouraged to facilitate the alignment of supervisory experience.
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)?	The developing nature of big data, analytics and robo-advice (as one single use case among many for the underlying technologies) is too new to determine precisely what data is required. Theoretically, as the AI learns it may become clear that different (whether more or less) data points are required to provide the best possible service. As such, any effort to set a minimum amount or the characteristics of information about the service user risks limiting the development of the technology and possibly the benefit available to the consumers. As other regulation relevant to the provision of financial advice or the use of data changes the minimum requirements could change with them. The regulations could then end up being inconsistent or even contradictory. In the case of financial advice this could have damaging consequences on the consumers. As it currently stands, services and regulation should rely on data that could allow FinTechs (Banks, non-banking FinTech/FinTech start-ups) to be compliant with existing regulation such as GDPR and financial markets regulation (e.g. suitability, KYC). Additionally, imposing minimum information requirements could restrict the ability to innovate and lead to homogeneous approaches that exclude a part of the users' base.
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?	Once again, it is important to highlight that there are other applications for big data analytics and artificial intelligence than robo-advice. These use cases could have substantial positive effects on consumers and the market including in the areas of enhanced cyber security and streamlined processes. Banks have been using data and analytics for a number of years and consider that big data and AI services will evolve according to consumer's preferences (e.g. Some consumers will likely prefer to interact with a human adviser, for example). Customer service is an area of intense competitive pressure and banks will therefore continue to attempt to provide a level of service that meets or exceeds customer expectations. It may be appropriate to consider any potential legislative initiatives in the light of technological advancements, but we maintain that the best approach to ensuring

		consumer protection is to regulate for the service and not the means by which this is provided. Please see the questions above for the reasoning behind this approach. ▪ With respect to consumer protection, some will consider that consumer protection challenges/risks related to artificial intelligence and big data analytics (e.g. robo-advice) could be the inability of customers to talk to a non-human adviser. It is however important to stress that although the characteristics of automated financial advice limit human intervention, an access to an operator (via an online chat, mail or telephone) may be provided to help the customer along the process. This issue is very important in particular where customer financial or digital knowledge is low. It may be sufficient that a human stands 'at the end' of every process. Of course AI and big data analytics can be used throughout, but human intervention must not be cut out completely. ▪ Considering that further evolutions in the use of Artificial Intelligence and Big Data are expected to emerge, the banking sector is currently assessing their applicability and the deployment of technological developments as well as the impact of existing and recent legislations on innovation and consumer protection. Indeed, several existing pieces of EU legislations and/or other regulatory requirements such as the Payment Services Directive 2, the General Data Protection Regulation (GDPR), the Markets in Financial Instruments Directive (MIFID 2), etc. are expected to mitigate potential risks which could be linked to the lack of transparency, misuse of data, consumers "locked-in" etc. For example, MIFID 2 is expected to lead to important changes in the organisation of consultancy services offered by banks to their customers, following the introduction of the new rules on consultancy (investment advice), incentives (inducement) and suitability assessment. The GDPR tries to create transparency for users (data subjects) who should be informed and should have the right to decline use of their personal data or withdraw their consent as well as a framework on the conditions under which profiling can be performed. ▪ Finally, cybersecurity threats remain one of the most important challenges for banks. As recently confirmed by Europol in the wake of the Wannacry ransomware attack, banks have made substantial progress on this front compared to other sectors of the economy. More needs to be done and increased cooperation among the regulatory and

		supervisory authorities at national, European and global level will enhance progress significantly on this front. At the same time, every provider handling financial data from consumers should have the same regulatory constraints, as the entire system can be by weakened by the weakest link. In our view, existing regulation already provides a strong level of protection and will continue to do so as the greater use of data in banking evolves. It is necessary, though, to make sure that the application of this framework is consistent throughout the EU and with all kind of players, making sure, especially, that customers are clear when advice is being provided or not. An issue to look into in the context of consumer protection is the legal liability of each actor involved in a given service (e.g. cognitive engine provider, system integrator that trained the machine, company offering the service, or the users themselves). As such, it could be argued that the best approach for ensuring consumer protection is for banks to take a risk based approach to mitigating and controlling for possible consumer protection risks.
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? **(Yes/No/Don't Know- not relevant)** 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.	**YES** We believe that national regulatory regimes for crowdfunding in Europe impact on the development of crowdfunding. In general, further harmonization of European legislation is needed. There are many different legal frameworks, several of which are outdated and not suitable for this type of digital financial service. As a part of the CMU, the aim should be to have a common EU-wide set of rules also for crowdfunding and other similar financing channels. The focus should also be on supporting equity crowdfunding rather than debt crowdfunding. Several national regulatory regimes for crowdfunding in Europe impact on the development of crowdfunding: ▪ **Finland:** Crowdfunding Act is in place since September 2016. The aim of the Act is to lower barriers to entry for new intermediaries (e.g. by lowering capital requirements, not requiring MiFID licence etc.). The law also aims to create a level playing field where players of different categories could compete on even terms. ▪ **France:** In France, public authorities adapted the regulations in 2014 to favour the development of participative financing in an environment protecting the contributors

		(donors, lenders or investors). A label was also created to identify those platforms which respect the new rules. According to the nature of the proposed financing, the participative financing platforms have to register or not with a regulated status depending on the type of activity and financing (loans, gift, subscription of Financial securities, etc.). The French Authority for prudential control and resolution Autorité de contrôle prudentiel et de resolution (ACPR))can check at any time an intermediary in participative financing. ▪ **Italy:** Special regulations on the use of equity crowdfunding platforms have been introduced in Italy and integrated with the MIFID regulations in order to protect the investor from making investments which, by their nature, are risky, and to make transactions - below certain thresholds - easier. The regulations have also been improved recently, but equity crowdfunding transactions have not reached the levels hoped for. ▪ **Ireland:** The Irish Department of Finance is currently consulting on Crowdfunding and possible need for regulation. There are numerous crowd-funders active in the Irish market and the Irish Government is assessing whether a regulatory regime would be appropriate for the crowdfunding sector, or if such a regime (or limited regime) with its inherent obligations and costs would be an impediment to the development of crowdfunding in Ireland. ▪ **Portugal:** In the specific case of Portugal, a law has been in place since 2015. Crowdfunding platforms operating in Portugal are monitored by the Portuguese Securities Market Commission (CMVM) (and have to be registered at the General Consumer Office. The law regulates four types of platforms: 1. collaborative funding through donation, by which the funded entity receives a grant, with or without delivery of a non-monetary contribution; 2. collaborative funding with reward, by which the funded entity is obliged to provide the product or financed service in return; 3. collaborative equity financing, whereby the financed entity pays the financing obtained through participation in share capital, distribution of dividends or profit sharing; and

		4. collaborative funding by loan, by which the funded entity pays the financing obtained through the payment of interest fixed at the time of the raising. There is still limited data available on the crowdfunding volumes. Nevertheless, it is clear the system is yet in its infancy so, an additional degree of caution is warranted, which underpins the investment limits enshrined in the legislation. ▪ **Spain:** Equity-based crowdfunding and crowdlending are regulated by the CNMV, and in the case of lending or models involving payments services, authorization by the Bank of Spain. Consumer protection is at the heart of this legislation and discriminates between accredited and non-accredited investors. Some critical points to note are the stringent limit to total capital raised (2 million euros) and limits to individual investment (3.000 euros per project and annual 10.000 euros per platform, for non-accredited investors). ▪ **The Netherlands:** The number of crowdfunding platforms has rapidly increased to more than one hundred over four years' time, covering about € 300 millions. According to the Crowdfunding Register of the Dutch Authority for Financial Markets ('AFM'), 13 platforms hold an AFM permit, meaning that the vast majority holds an exemption. Unfortunately, many platforms communicate on a very minimal level about financial risks, where the risks are often significant. The consultation document seems to suggest that there are only two permit categories: a temporary or a permanent permit. In the (Dutch) practice, we see that the market needs a growth-model, where regulation is being adapted to the specific event in place (test phase, client scale up, and offering particular services). ▪ **UK:** The FCA's current rules on loan-based and investment-based crowdfunding platforms came into force in April 2014. The focus is ensuring that investor protection levels are appropriate for the risks in the crowdfunding sector while promoting effective competition in the interests of consumers. Consultation is ongoing on more prescriptive requirements on the content and timing of disclosures by both loan-based and investment-based crowdfunding platforms. - For loan-based crowdfunding there are also consultations on: - strengthening rules on wind-down plans - additional requirements or restrictions on cross-platform investment - extending mortgage-lending standards to loan-based platforms.

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?	Non-bank financing platforms and companies should also be given a regulatory framework to enhance trust of customers in such solutions and foster a competitive market with similar basic rules. This should ensure that the necessary consumer protection measures are in place, irrespective of the provider. The Commission must always apply the principle of "same activities, same rules and same supervision" in order to ensure consumer protection and market integrity. Although in recent years several harmonization initiatives already took place, namely Payment Services Directive 2 (PSD2), MIFID, Peer-to-Peer lending initiatives are still in an early stage, warranting further alignment between members states, namely: ▪ criteria and requirements for registration of as a crowdfunding platform, distinguishing between reward based, donation, debt and equity financing; ▪ capital requirements; ▪ continuity requirements; ▪ criteria for investors on-boarding in a crowdfunding platform, namely non-accredited and accredited investors; ▪ collection of non-performing loans (debt crowdfunding) ▪ Framework for active partnerships - banking financing and crowdfunding platforms (e.g. partial financing by a bank loan, partial financing by a crowdfunding platform); ▪ criteria and requirements for effective credit score assessment and embedded insurance protection services in order to correctly inform and protect the individual investor correctly. One additional way would be the institutionalisation (especially regarding lending) of "go-between" structures/vehicles between end-customers and credit institutions with potential benefits to all parties involved. The subject of supervision of platforms granting credit should be revised at European level with the aim of a wider convergence of registration and supervision practices. Regarding the granting of credit, the principles of the analysis of solvency are framed by the European Directives on mortgage credit (MCD) and consumer credit (CCD). It is important to ensure that they are properly implemented, including by new participants bringing innovative models, to protect the consumer against the risk of over-indebtedness. Certain regulations and guidelines only cover credit institutions. Certain specialized or alternative

		platforms are not supervised in the same way, creating distortions that hampers strong consumer protection.
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?	Financial crowdfunding platforms, and particularly peer-to-peer platforms, operating with products akin to financial ones, tend to carry out their activity with greater informality and lighter regulation, thereby increasing potential solvency risks. This exacerbates problems of information asymmetry between funding suppliers and those requesting it. Consequently, we believe that there must be a compulsory and specific regulatory framework laying down a **minimum set of disclosure information, risk factors, data transparency, use of proceeds, and harmonisation of required information**. This would be put in place in order to protect and correctly inform the individual investor. Transparency in this context is important regarding fraud, money laundering, terrorism financing and new regulations governing these areas such as MiFID 2. On the other hand personal data must be secure and protected. There should be no risks to the rights and freedoms of people that could occur due to transparency reasons, except for compliance with legal obligations, which may occur frequently especially in the context of transparency in regard to financing options like crowd-funding.. Self-regulatory initiatives are a good tool to develop innovative solutions. However we do not believe that self-regulatory initiatives are sufficient. Rather it makes it difficult for supervisors and the wider market to understand the minimum levels of protection and transparency undertaken by such entities. This also has an impact on investor/consumer perception and the subsequent ability of such players to scale up. Rather a harmonised approach at EU level is required. Lending, crowdfunding and invoice trading platforms should periodically publish their registered default rates and have clear conflict of interest policies. European legislation could also establish a rating of the crowdfunding platforms on the basis of the transparency levels adopted.
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?	Sensor data analytics and, in general, big data technologies, are changing the provision of insurance and other financial services as new sources of data, alternative data, can be taken into account for risk scoring, pricing and for the provision of tailor-made products. The lack of security standardization in the Internet of Things (IoT) and sensor data analytics is an example of a real challenge we are seeing nowadays and on which the EC and other regulators are beginning to be concerned. IoT manufacturers should increase security measures to protect data. There is also a lack of consensus on the security standards to be used among manufacturers or among countries like China, USA and Europe.
1.10	Are there already examples of price discrimination of users through the use of big data? **(Yes/No/Don't Know- not relevant)** Please provide examples of what are the criteria used to discriminate on price (e.g. sensor analytics, requests for information, etc.)?	**DON'T KNOW- NOT RELEVANT** As regards price discrimination in a negative sense (with ethical implications, like taking into account variables that could have moral implications), we consider that there is not enough evidence on the market to provide examples. Charging different prices to different individuals for the same product or service has been a common practice since old times. Pricing practices take different forms and evolve over time. Such pricing practices need not always be a concern but only when they are discriminatory with no objective foundation. Any assessment of pricing practices should be specific to the product and market in question. Furthermore, it is not the form of pricing that matters but rather the effect on consumers or consumer perception. The effect of such pricing depends on the market context. There is a need of an assessment on a case-by-case basis to avoid the risk of identifying the problem incorrectly and proposing an inadequate solution.
Other technologies that may improve access to financial services		
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	Technologies which allow financial services to be activated remotely and accessible via digital channels (e.g. videoconferencing for client on-boarding, geolocation to fight payment fraud, biometrics to simplify customer on-boarding process and authenticate transaction). Or technologies which make the purchasing process simple while still providing guarantees for the parties involved, central to the innovation being pursued by banks. While some technological advance may open products to whole new groups of customers (e.g. robo-advice discussed above), others may simply streamline existing

	that you consider particularly innovative?	processes making it easier for consumers to carry out their banking tasks. In this sense, behavioural biometrics is a promising field that will allow for a seamless user experience that preserves a high level of security. Regulations could be improved to assist these technologies and take into consideration, for example, biometric technologies to sign contracts, to simplify UX, authentication and identification; real time payments improve customer experience and increase efficiency. These should not be overlooked as more efficient and effective processes open opportunities for banks to innovate from which more significant improvements to the customer experience may develop. Technologies that help banks correctly and securely identify their customers both remotely (over phone/chat/email) or in person could greatly help the usability of financial services and ease processes within the banks. ▪ **Cloud computing** is the area that requires the most urgent attention from EU regulators and policy makers. This will be developed in more detail in later answers, however it should be underlined that a significant amount of the new technologies discussed in this paper are best operated from a cloud environment. Thus encouraging and streamlining the use and application of cloud computing in banking and financial services is essential to increase the level of innovation and technology change taking place in the industry which in turn will benefit consumers and strengthens markets. Cloud computing is essential for data analytics in particular. The increased computer resourcing provided by cloud enables the processing and analysis of data on scale which can produce real benefits for consumers like those discussed above. ▪ Moreover, the use and application of **Distributed Ledger Technology and "Smart Contracts"1** can potentially enhance specific businesses of the Bank (e.g. trade finance) and general areas (e.g., IT core banking) and could be considered as innovative. These programmable digital contracts can self-execute, self-enforce, self-verify, and self-constrain the business logics "described" by their code, relying on the underlying blockchain protocol to communicate, compute and validate the transactions, while maintaining/updating the distributed ledger shared by every network participant. In this latest version, blockchain and smart contracts have the

[1] Smart Contracts are self-executing pieces of codes translating contractual terms into computational material. ESMA's Report: The Distributed Ledger Technology Applied to Securities Markets.

		potential to trigger far-reaching changes in banking processes. Blockchain could do to finance what the Internet has done to communication: it opens the doors to a new financial paradigm, which is now defined as Crypto Finance. However, it is still early days and it is difficult to predict where the technology will take the banking industry and which products and processes will be affected. Currently, the development is changing rapidly. ▪ **Big data analytics and Artificial Intelligence** are technologies with a great potential to further expand access to financial services further by lowering for example, the complexity and the costs associated to certain advisory and credit scoring services. ▪ **Digital Identity**: verifying and safeguarding identity has always been a core part of banking. This is not to say that banks should be the sole providers of identity platforms; quite the contrary. However banks can supply their expertise and infrastructure. ▪ Finally, the **combination of digital identity and blockchain** has palpable potential in a number of banking areas. Most notably, banks are keen to pursue with regulators potential AML and KYC solutions which could be enabled by this combination. ▪ Although a **digital platform** is not a disruptive technology itself, this innovative business approach makes use of available technologies such as the public cloud or mobile technology to reduce information asymmetries and expand markets. Finally, there is also an opportunity in the use of technology to improve financial literacy among European citizens. Greater access to financial services might be achieved by acting on the demand side as well as on the supply.
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?	Some of the most promising use cases of FinTech to reduce costs and improve processes among our members are: ▪ robotics to reduce costs by re-framing existing processes to End to End processes ▪ trading platforms that reduce costs while increasing markets transparency;

		▪ distributed Ledger Technology/blockchain could be a technology which assists the processes between parties who need to improve the information exchanged, particularly where no trusted central dedicated infrastructures exist. ▪ platforms used in Capital Markets to access data in a simpler and more efficient way; ▪ digitalization of processes that facilitate the interaction with customers ▪ AI/Big data use to improve the focus of resources and sales on the right customers at the right time (which customer needs which product at which period of his life) including universal multilingual transactional BOTs where the transactions are made by the use of Artificial Intelligence from and to any language. ▪ robo-advice to leverage sales in retail with better/more sophisticated products with lower costs. Indeed robo-advisory is mostly intended to give automated financial advice so as to allocate, manage and optimize clients' assets automatically; ▪ costs can be significantly reduced, and processes improved, in the field of regulatory compliance and reporting. So-called Regtech can be considered as a subset of FinTech aiming at the resolution of exactly these issues; ▪ biometric authentication technologies (to accelerate all on-boarding, digital signature and even KYC processes); ▪ Application Programming Interface economy (API) models (to leverage X2X solutions where X can be B-business, C-client and M-machine) and Machine Learning powered models (for risk, knowledge, language, etc.); ▪ cloud computing allows for greater scalability and flexibility to innovate, and it is behind the recent "APIfication" trend, whereby infrastructure, platforms and data services can be offered to internal or external developers in an extremely convenient way. Further collaboration with FinTech Start-ups/non-banking companies is expected to take place. However, 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 engaging with innovative

		start-ups that do not have the resources or the expertise to develop risk control frameworks excessively complex for banks. 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 EC's first and foremost role is to develop a framework which facilitates innovations to thrive in the Digital Single Market which understands and embraces the profound transformation that the financial services industry is facing. This market-driven approach has of course certain shortfalls, hence the EC should ensure that Europe's geostrategic autonomy and economic continuity is preserved, and should promote European commercial alternatives in critical services such as cloud computing. It should ensure that the European legislation framework is sufficiently competitive in an international environment. ▪ **Level playing field:** a prerequisite is to ensure that consumers are protected and financial stability ensured, irrespective of who provide the service.As a result , it is necessary to maintain a level playing field regarding regulation across potential competitors/sectors and Members States (addressing issues such as KYC, digital on-boarding, electronic signature of operations, capital requirements, MiFID etc.). ▪ **Cloud computing :** The EU could play a role: - **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. These constraints also create significant frictions in ensuring that regulatory compliance is achieved in contractual negotiations between banks and cloud service providers (CSPs). - **Further harmonising of regulatory approaches across different jurisdictions**. 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 uncertainty created by the variation in approach reduces the appeal of the EU as a place to do business.

		This is not unique to the incumbent banking industry, New FinTech start-ups, and neo-digital challenger banks, many of whom are cloud native, will experience barriers to growth as a result of the lack of harmonisation across the EU. Finally, harmonising approaches to the cloud across jurisdictions will also help to facilitate the adoption of cloud at a global level which creates efficiencies and encourages growth. - **Clarifying further the requisite uniform methods with which the banking sector has to comply in order to assess and ensure adequately security and privacy**, not least to maintain trust and confidence of the financial system. If privacy and security measures are breached, this would have a serious negative impact for customers and for financial institutions. - **Establishing appropriate technical and organisational safeguards:** Global IT solutions may be a great measure to facilitate compliance by banks and safety for customers. - **Facilitating the cloud adoption process and reducing time to market to increase competitiveness**. - **Supporting the creation of a clear and consistent regulatory framework at EU and Global levels, and guaranteeing a proportionate risk-based approach** to due diligence and contracts between the Cloud Servicing Providers (CSPs) and the banking sector in respect of Cloud Computing in Financial Services. ▪ **Cybersecurity:** this field is key in order to continue exploring new technologies and scenarios that can reduce cost and risks such as cyberattacks, data leaks, etc. This can be achieved by individual efforts from companies and from collaboration with other market players such as FinTech start-ups, cross sector companies, vendors and providers, regulators/supervisors and law enforcements. The EU could play a role in: - **streamlining harmonised format including definitions and procedures for security (IT) incident reporting** to avoid overlap and redundancy in reporting

		to multiple competent authorities (NIS Directive, PSD2, Data protection regulation, Single Supervisory Mechanism SSM)). - **establishing, for resilience purposes and risk mitigation establishing a legal framework for data sharing** which allows the possibility of sensitive information related to fraud & cyber-attacks at national and cross-border level to be put in place. - **Improving the current collaboration between the industry and regulators and among regulators.** This would help to overcome the regulation challenges and maintain the speed of innovation / digitalization. The public sector needs to work proactively with the private sector, across borders, to share information about attacks, exchange best practices and continually improve security systems to deter cyber criminals - **extending the legal framework to all players that use financial data to avoid that weakest link endangering all the systems;** - **In certain cases and due to current legal constraints, allowing the exploration of new solutions via a framework of experimentation where product and services can be tested.** Indeed, others might explore new scenarios such as fraud prevention via AI and Big Data techniques based on behaviours patterns and cyber intelligence gathering of personal and non-personal information. ▪ **Indirect support (Skills and procurement):** developing and acquiring the right digital talent and skills within the EC is the best way forward for European policy making to keep pace. Moreover, the EC has another lever in its public procurement strategy and should use it to promote European solutions whenever the domestic offering is comparable to foreign alternatives. ▪ **Automated financial services** (See above)
2.3	What kind of impact on employment do you expect as a result of	Automation and innovation do not necessarily mean a reduction on overall employment as digitalisation is expected to create demand for new skills and competences. Firms in

	implementing FinTech solutions? What skills are required to accompany such change?	the financial industry will face the challenge to find suitable (i.e. more or differently qualified) employees for new creative jobs by attracting new talents and re-skilling/up-skilling existing employees. FinTech is likely to create greater dispersion in financial services-related employment. Incumbents will not increase their headcount to remain competitive in a more dynamic environment, while new entrants will need to recruit experienced professionals to deliver innovative value propositions. Some of the most traditional activities in banking will be made redundant by technology, but other specialised jobs will be created to accomplish the digital transformation of the industry. Therefore, emphasis should be placed on digital skills and a profound change in mind-set. Collaborating with non-banking FinTech/ FinTech start-ups will further enhance the industry's open-mindedness, adaptability, fast execution and long term view. It will also introduce new skills and new company culture, enabling new working methodologies (e.g. design thinking, Scrum, Agile, data science, business development, IT, user experience and finance, etc.). Employees with specific competences in ICT, science, technology, engineering and mathematics are likely to be required. Banks will need to implement large-scale career re-orientation programmes for their personnel, in order to respond to the new digital age. Furthermore, not only firms, but also social partners, policy makers and supervisors will have to adapt their related frameworks to this new digital environment. It is important to note that the current prudential requirements imposed on banks constrain the variable remuneration that an employee within a bank can receive (not to mention other rules such as the deferral of payment or part of the payment in instrument of the financial institutions etc.). This restriction affects digital specialists who do not perform risk taking (including operational risk) activities but who are essential for the digital transformation. Therefore, we see that financial institutions/banks tend to compare less favourably in the labour market with the digital environment where innovators tend to be remunerated with equity participation that encourages entrepreneurship. Consequently, it is extremely difficult to attract and retain scarce digital talent when banks cannot offer packages that compete with those offered by their digital peers, which in turn undermines the creation of a level-playing field.

		To resolve this issue, remuneration rules should be applied in a proportional manner so 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.
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 manage the regulatory environment, allowing them to be more efficient and dynamic in their response to new requirements and expectations. The most promising use cases of technologies for compliance purposes are listed below. ▪ **Know Your Customer/ Ultimate Beneficial Ownership platforms leveraging on breakthrough technologies.** ▪ **Cognitive technologies applied to: mapping of regulations/policies and its consequent impact assessment, transaction monitoring, market abuse and trade activities.** ▪ **Automation of compliance reporting.** ▪ **Anti-Money laundering/ counterfeiting the Financing of Terrorism/ Financial crimes/ Cybercrime (e.g. Databases of mule accounts and fraudulent websites, phone numbers, e-mails, etc.).** ▪ **The application of data analytics and so-called "big data."** These techniques can be used to reduce compliance risks in areas such as anti-money laundering. Big data techniques can identify potentially high risk customers (possibly in combination with biometrics to identify a client in a digital environment and/or authenticate a high risk transaction); make reporting information more accessible and easily searchable to regulators; improve internal culture and behaviour by better identifying actions that could lead to compliance violations or incur reputational risks to the institution; and in combining big data with artificial intelligence, allow firms to reduce market risk through

		more precise modelling and forecasting of market trends and sentiments. Control and evaluation can be done more effectively via AI in the future. Using robots (virtual, but also physical ones) can improve quality as well as quantity of regulatory control and, as a result, lower risks. ▪ **The area of distributed ledger technology (DLT),** was initially popularised through the exchange of the digital currency Bitcoin. However, DLT may have many potential applications beyond digital currencies, many of which are relevant to the financial services industry. 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 between financial institutions and regulators. Properly developed, it can lead to a win-win situation for financial institutions and regulators, allowing firms to reduce operational costs and providing regulators with greater transparency and risk reduction in the financial system. (e.g. via the development of a proper business case at banks and industry level). ▪ **The growing use of encryption** has the potential to reduce cybersecurity risk by creating another layer of security to deter unauthorised access to data. Regulators have pointed to cyber-risk as one of the most important threats to financial stability. Firms, however, need time to expand the use of encryption, particularly to legacy data systems, as well as discretion to determine what information is material, given the voluminous amount of data a typical financial institution holds. ▪ **The introduction of biometrics for the identification** of clients, following KYC/ AML/ CFT legal requirements, which improves 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 as well as laws and regulations. It can also contribute to a better compliance of the customer protection processes. Moreover, due to the fast regulatory change it is difficult to keep apace in order to comply. These technologies can also allow the correct identification, interpretation and allocation of the

		responsibilities which are currently a labour-intensive and complex, as well as very often very slow, process. Tools to improve the automated interpretation of regulations are a key asset in this environment. It is necessary to speed up innovation in the banking sector and address and overcome banks' concerns in terms of adopting RegTech solutions. Thus all aspects of compliance must be resolved assuring an effective time to market to Banks and FinTech start-ups (e.g. collaborative compliance, framework of experimentation). Regulators should take a more proactive approach in this regard. 1. At a minimum, this means an expertise build-up and creating forums for open discussion of RegTech/ FinTech issues. It is important to involve regulators, financial institutions, technology companies, and RegTech ventures: - To facilitate the creation of new RegTech solutions by authorising the use of new technologies for these purposes (e.g data protection); - To enable a safe environment to share sensitive information between the industry and its supervisors. 2. Reduce the regulatory uncertainty (due in part to the still unfinished regulatory agenda) and harmonise the procedures and standardise information demanded by different authorities via an EU framework of experimentation with an exchange of good practices and where RegTech will be closely monitored in a safe harbor, regulatory environment. 3. 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. 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?		

2.5.1	What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services?	There are several obstacles to the adoption of cloud computing solutions by the banking sector: ▪ **The lack of harmonisation in regulatory and supervisory approaches across different jurisdictions for the adoption of the cloud.** According to the financial rules on outsourcing for many EU countries, financial institutions must notify the supervisor and obtain their approval to launch cloud projects. This notification and approval has to be done on a case by case basis. It implies an indirect constraint to the free flow of data and, thus, to a faster innovation and a more agile cloud adoption. The variation in approaches to cloud computing in financial services by various national regulators creates inefficiencies, particularly for banks operating with a global presence and global customers. It reduces the appeal of the EU as a place to do business and to meet the objectives of the Capital Markets Union, Digital Single Market and cross-border business. This is not unique to the banking industry, FinTech start-ups, and non-banking FinTech, many of whom are cloud native, will experience barriers to growth as a result of the lack of harmonisation across the EU. There is a need to harmonise EU financial supervisors' criteria when approving cloud projects. Harmonising approaches to the cloud across jurisdictions will help facilitating the adoption of cloud by financial institutions at a global level which creates efficiencies and encourages growth. ▪ **Existing regulation and domestic laws which establish barriers to the geographic location of the physical Cloud Computing infrastructure.** - Frictions to leveraging the benefits of Cloud Computing in Financial Services arise when data regimes restrict cross-border data flows, both within the EU and globally. Data stored in a Cloud Computing environment can be fragmented geographically and its support functions (such as processing, hosting, backup, support and management), divided among suppliers (often across national boundaries) to enhance their data security, disaster recovery and resilience. In this regard, this progress in technology towards a 'distributed' network infrastructure challenges traditional data and outsourcing concepts such as the physical data localisation and auditing of physical premises.

		- We observe that several EU countries have introduced, at national level, additional limitations and barriers which prevent data circulation and intra-group synergies at EU and international levels. These have an impact on risk management, centralised/ shared infrastructure strategies, and the ability to provide products and services to global customers. Banks need to be able to transfer data across borders efficiently so as to respond to customers' needs: delivering goods and services, processing payments or providing customer support. To achieve cross-border data flows, there must be no direct or indirect restrictions on data localisation. Limiting data flows without objective and justified reasons undermines the ability of companies to define their business models; it will be detrimental to competitiveness and growth of EU companies; and, endanger the functioning of critical infrastructure. We would argue that whilst Member States' interests in national security and law enforcement are fully legitimate in most cases (not least those linked to non-personal data), there is no valid justification for data localisation. In practice, these interests are too often used to justify, largely unrelated, measures. - We agree with the Commission's statement that localisation restrictions rarely advance the public policy objectives they are intended to achieve. The EBF fully supports any EU initiative that could remove restrictions to the free flow of data which at the same time acknowledges the right that businesses have to choose where they store their own data. Companies' decisions on data localisation may be part of a specific business model and companies must be allowed to request or provide data localisation. This is a choice made by both providers and recipients of the service, which is quite different from a legislation obligation to do so. ▪ The current regulatory / supervisory framework governing outsourcing is also a major obstacle to the greater use of cloud computing services by financial services firms. See responses to questions 2.2 and 2.10.

		▪ **The lack of clarity on the requisite uniform methods with which the banking sector has to comply in order to assess and ensure adequately the security and privacy:** - Requirements under the GDPR raise risks in relation to personal data. In particular, 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 vendors. However, the reality of cloud infrastructures makes compliance with GDPR very difficult. 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. This is a significant barrier for banks entering wholesale into the cloud and is likely to inhibit the use of FinTech companies that offer innovative cloud solutions. These constraints also create significant frictions in ensuring that regulatory compliance is achieved in contractual negotiations between banks and cloud service providers (CSPs). - There is also legal uncertainty with the contracts (Privacy Shield, MCC and BCR) used to transfer data outside the European Union which needs to be solved. The Article 29 data protection Working Party states that certain countries are not complying with the Data Protection requirements and these contracts might be declared illegal in the near future. - There are also certain overlaps in relation to data protection measures to be taken, between the European Central Bank and the national data protection authorities. ▪ There is a need to **bring agility to the cloud adoption process, reducing time to market to increase competitiveness.**
2.5.2	Does this warrant measures at EU level? **(Yes/No/Don't Know- not relevant)**	**YES** ▪ In order to support and facilitate a responsible adoption of cloud computing within the banking industry, the European Commission should focus on efforts that support the creation of a clear and consistent regulatory framework at EU and Global level, and

	Please elaborate on your reply to whether the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services warrant measures at EU level.	guarantee a proportionate risk-based approach to due diligence and contracts between the Cloud Servicing Providers (CSPs) and the banking sector in respect of Cloud Computing in Financial Services. Also, governments should help facilitate the conditions to allow the insurance industry to engage in this area. The use of insurance mechanisms would encourage financial organisations to use cloud services on a larger scale. ▪ It would be very useful to establish a common cloud risk framework across the EU to evaluate and mitigate risks of data and services transfer in the cloud, tailored on the different service and delivery models, which could help companies to evaluate risks on the same criteria adopted by cloud service providers (CSPs). Based on the risk framework, a common set of rules should be defined, appropriate to each sector's needs, with a certification scheme set up by supervisors within the EU. This would help CSPs certify once for each sector. In particular, it would help banks to have the assurance of compliance to the banking requirements and help supervisors to accept certifications as a proof of due diligence, reducing the burden of multiple audit activities. Certification Schemes and the European Commission's "Cloud Certification Schemes Metaframework (CCSM)" should be welcomed as well as the standards promoted by the NIS Directive. The CCSM maps out detailed security requirements used in the public sector to describe security objectives in existing cloud certification schemes. However, a step further should be taken to coordinate the development of sets of certifiable controls (interesting in this regard is the work carried out by the Cloud Security Alliance as part of the STAR certification and the SSAE 16 type II, which is an internationally recognised standard to audit on security and governance.) Specific certifications, like PSD2 requirements adequacy, would help increase liability for specific scopes like payment. For example, the audit should be performed by an independent third party, and should be accepted by supervisory authorities as a guarantee of regulatory compliance and real implementation of the recognised measures and controls. Thus, banks subscribing to the audited cloud service, would be able to rely on these audit results without having to carry out their own audit. Nonetheless, it must not preclude banks from keeping their contractual audit rights, to be activated on a case by case assessment of the risks. Indeed, banks need to

		assess, depending on the result of the due diligence, whether they need an external audit by an independent third party or whether they can audit directly. Also, a harmonised approach to defining the level of access to the business premises of the CSP, that need to be contractually secured by banks, should be taken by European Supervisory Authorities and National Financial Supervisory Authorities and clearly communicated in order for the CSPs to be able to adopt their offering to the banking sector in accordance with such requirements. Regulators should be directed to undertake greater analysis on how extensive auditing of suppliers in the supply chain should be, in order to provide banks with a better understanding of how to ensure regulatory compliance through exercising a proportionate risk-based approach. ▪ 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. ▪ 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. ▪ It is also essential to update the EBA (European Banking Authority) Guidance on outsourcing, which dates back from 2006. It needs to be adapted to the cloud computing technology. Any EU initiative that could remove restrictions to the free flow of data which at the same time acknowledges the right that businesses have to choose where they store their own data should be strongly encouraged. Companies' decisions on data localisation may be part of a specific business model and companies must be allowed to request or provide

		data localisation. This is a choice made by both providers and recipients of the service, which is quite different from a regulatory obligation to do so.
2.6.1	Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with? **(Yes/No/Don't Know- not relevant)** Please elaborate on your reply to whether commercially available cloud solutions do meet the minimum requirements that financial service providers need to comply with.	**YES** This varies widely between service providers. Some of the more mature service providers have made progress in offering terms which enable financial services firms to comply with the applicable regulatory / supervisory framework. However, other service providers fail to accommodate these requirements. Overall, the position is that financial services firms have difficulty in finding public cloud based solutions that enable them to clearly comply with the applicable regulatory / supervisory framework. The solutions (the big CSPs) need to meet the requirements, because banks have to make sure that cloud solutions proposed are compliant with the supervisory requirements; otherwise banks would refuse to adopt the cloud solution. The big CSPs do comply at least from the point of view of security with international recognized standards such as ISO 27001, NIST, PCI, and even have SOC2 reports based on SSAE 16 to ensure compliance. Nonetheless, it is not the case for all European CSPs, some of which may not be in compliance with these security standards. Usually, there is a problem to comply with the right to audit as required by the ECB. CSPs that comply with such standards facilitate it, as it would make it easier for FinTechs and banks to comply with the supervisor (we would not have to negotiate it in every contract). Uncertainties pertaining to compliance with certain regulatory requirements, such as outsourcing requirements regarding effective supervision and oversight of CSPs and supply chains, challenge a proportionate risk-based approach to due diligence. Under existing outsourcing requirements, banks are required by national supervisors to have internal controls in place which achieve effective identification, monitoring and reporting of risk in terms of data protection, business continuity, etc. This includes not only undertaking initial and ongoing due diligence of the CSP, but also of those service providers within the supply chain. It means that when entering into a cloud arrangement, banks must ensure that the arrangement with the CSP does not materially impair their ability to comply with the supervisory requirements or the ability of a regulator to monitor a bank's compliance with its regulatory obligations.

		Banks have to make sure that the CSPs meet the same requirements for data security and quality of service but also comply with the supervisory requirements imposed on banks. Banks then 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. 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. However, It leads to difficulties when switching Cloud Service Provider due to heavy regulatory requirements that banks have to adapt too (and CSPs have to consider) and because the contractual conditions are often difficult to change and adapt to the country of use. The issue related to the complexity of auditing outsourced services to the cloud has long been known. Banks are required to cooperate with regulators, and generally secure (on-site) access rights to records, premises and personnel. However, the physical access to premises hosting the cloud infrastructure is often a point of tension in negotiations with CSPs, who may be reluctant to allow customers into their data centres for legitimate security and confidentiality reasons. Furthermore, in a globalised and distributed cloud model, access to the physical location delivers a negligible outcome, other than the most basic one of physical security and access checks. In contrast, a virtual audit of data can be of much greater relevance to ensuring appropriate controls are in place. Complex supply chains such as a SaaS solution built on another provider's infrastructure/ platform also make securing rights to have access/ to interview personnel (for each party of the supply chain) challenging in negotiations. Effective identification, monitoring and reporting of risk is thus more challenging in many cloud environments given the lack of visibility over the whole supply chain of the technology stack. This challenge is further driven by an ambiguity concerning how far auditing rights should be exercised throughout the supply chain. Without clarity concerning what is required to comply with regulatory requirements, banks may either look to secure rights extensively all the way down the supply chain, or may, on the other hand, be forced to take on additional risk in not securing extensive audit rights.

		The challenge for cloud providers is compounded by the large number of customers and by the standardised offering which leads to a high level of complexity when giving individual customers the right to audit. As a result, effective identification, monitoring and reporting of risk is more difficult in many cloud environments given the lack of visibility in the whole supply chain of the technology stack. Besides the CSPs' operative responsibility around service provisioning, banks as data controllers are liable for the data stored and processed. As such, cloud service consumers need assurance that all contract terms are fulfilled. However, some CSPs are not always able to comply with specific contract terms, such as the right to audit.
2.6.2	Should commercially available cloud solutions include any specific contractual obligations to this end? **(Yes/No/Don't Know- not relevant)** Please elaborate on your reply to whether commercially available cloud solutions should include any specific contractual obligations to this end.	**YES** See response above Cloud solutions are a special IT contract that blend technology provision and outsourcing services. Therefore, contracts governing cloud services should be drafted in accordance with the applicable financial regulation without imposing further specific requirements. In our views, commercially available cloud solutions should include specific contractual obligations that facilitate the compliance with the different requirements that the financial supervisors impose to banks when migrating to the cloud. A template for an homogenous "basic contract form", which includes minimum regulatory provisions for cloud services (based on the existing financial regulatory framework), could help the banking sector to guarantee the regulatory compliance when migrating to the cloud. Also, this could help the Cloud Service Providers to adapt their offer while further helping the Financial institutions to better negotiate the specific conditions on the basis of a common scheme approved by the regulators. In this regard the EBF welcomes the objective of the recent consultation of the European Banking Authority to set up recommendations on the use of cloud computing which aim at clarifying the EU-wide supervisory expectations if institutions intend to adopt cloud computing, so as to allow them to leverage the benefits of using cloud services, while ensuring that any related risks are adequately identified and managed.
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?	We agree with the list of the potential applications of DLT in the Financial Services sector listed on page 11-12 of the EC FinTech Consultation. However, here are numerous other potential applications too, which have been widely publicised, for example, cross-border Trade Finance, Supply Chain Finance, Identity Management, KYC, Bank Reference Data etc. Some concrete examples include: ▪ **Digital Trade Chain (DTC):** A number of banks are partnering on a new blockchain-based trade finance platform for managing and tracking domestic and cross-border Open Account trade transactions securely. This platform aims to change the way SMEs view Open Account trade by making it paperless but secure and easy to use. DTC represents a simple, fast, efficient and secure way for customers to digitally initiate and track their trade transactions, and request selected banking services at the same time. ▪ **Utility Settlement Coin (USC):** A number of banks have been working on the concept of the Utility Settlement Coin an asset-backed digital cash instrument implemented on distributed ledger technology for use within global institutional financial markets. USC would be a series of cash assets, with a version for each of the major currencies (USD, EUR, GBP, CHF, etc.) and would be convertible at parity with a bank deposit in the corresponding currency. Unlike cash held as a commercial bank deposit, USC would be fully backed by cash assets held at a central bank. Essentially, spending a USC would be spending its paired real-world currency. The roll-out of the Utility Settlement Coin would basically mean the introduction of a common unit of value across different blockchain platforms in institutional markets. USC could have a wide range benefits from balance sheet implications to improved processes around clearing and settlement. Through having a digital cash instrument, linked to central bank money, the risk, complexity and time taken to settle and clear trades could be significantly reduced. ▪ **Real Time Payments**: Today the financial industry relies on a network of correspondent banks that allow payments to be made cross-borders on average on a T+1 / T+2 basis (though this timescale can extend especially if there are

		compliance/legal rules to follow e.g. because of the country of the payee). A number of banks have been reviewing new blockchain-based payment protocols available on the market like Ripple and experimenting with a proof of concept platform based on Ethereum. These solutions take advantage of the capabilities of blockchain to execute payment obligations netting and enable real-time clearing without the involvement of correspondent banks on each transaction. The DLT can provide **a single source of information** where SMEs can share their financial data (obviously complying with existing regulation, starting from GDPR) in order to help the financial institutions to assess their credit risk more effectively. This could make it easier for SMEs to access some banking services and especially financing services. It **could materialise via "Smart Contracts"** - contractual clauses to be fully self-executed, self-enforcing, or both, used in highly standardised operations. In trade-finance and in invoice prepayments, there are interesting applications supporting companies and SMEs. DLT use cases in Trade Finance **can help European SMEs increase their trade activities by making their domestic and cross-border commerce easier**. A DLT use case on Trade Finance could seamlessly connect the parties involved in a trade transaction (i.e. buyer, buyer's bank, seller, seller's bank and transporter) online and via mobile devices. This DLT use case would simplify trade finance processes for SMEs by addressing the challenge of managing, tracking and securing domestic and international trade transactions. Larger companies use documentary credit as a way of reducing the risks involved in doing business, but documentary credit is not always suitable for SMEs or for companies that prefer open account solutions. By maintaining secure records on a digital distributed ledger, Trade Finance use-cases will accelerate the order-to-settlement process and decrease administrative paperwork significantly. The transparency feature that a DLT platform's end-to-end provides, can give SMEs confidence to initiate trade with new partners in their home market or in other European markets. Other possible applications might be: ▪ B2B payments instantaneously settled;

		▪ cash pooling solutions; ▪ FX markert makers based in blockchain; ▪ Businesses where clearing and the need of independent third parties is crucial; ▪ Credit products such as factoring/Confirming or in the field of collections; ▪ In order to increase SMEs financing there could be the creation of a receivables repository on a blockchain/DLT, allowing banks to verify that a receivable has not already proposed to other banks for financing. Finally, it is important to underline that DLT applications for SME might have a direct or an indirect effect: ▪ Directly - (local and cross-border) invoice financing - this could grow exponentially once the financed invoices are identified/ marked over DLT (when coupled with counterparty identity and credit risk attached to the invoice), and would also be trading in a secondary market; ▪ Indirectly – due to streamlined/ improved financial reporting, covenants monitoring and securities issuance over DLT: - Equity funding, - Dynamic/ unsecured credit. Disruption in any of these specific areas could result in enhancing access to finance for enterprises. This disruption is not limited to DLT, though DLT has been a catalyst for re-thinking many of these existing business models. As such, DLT itself will meet the objectives of enhancing access to finance for enterprises. However, DLT may well result in disruptive changes to some of these business models that will meet the desired outcome. The underlying technology may include DLT, or selected parts of DLT to enable these business model changes.
2.8	What are the main challenges for the implementation of DLT solutions (e.g. technological challenges, data standardisation and interoperability of DLT systems)?	Currently it is extremely difficult to assess thoroughly the impact of the blockchain/DLT in financial services. However, it seems clear that such new technology would have a **strong impact on costs in renewing technology** and it **would lead to a deep reshaping of training, processes, standards and business models** (to mention only some of the most important areas impacted). On the other hand, it can create clear cost

		savings. For such reasons 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) should be addressed. In parallel, a **solid business case should be built** to understand which are the conditions upon which the use of such technology would create value foreach use case. In our answer we try to identify some of the issues that, we believe, the nascent technology will have to face and resolve before being considered as mature. It includes looking both at the governance and the technological needs. **Governance and privacy needs** ▪ **Governance framework**. The DLT that is likely to be applied to financial services would be 'permission-based' in contrast to a 'permissionless' system (like Bitcoin) for efficiency, security and privacy reasons. A permission-based framework requires rules to approve/ reject authorised participants, including perhaps minimum capital requirements, conduct of business rules and risk management processes. In addition, rules to govern the interactions between participants, both 'permissioned' and 'non-permissioned' will be necessary. Examples include the liabilities of the respective participants, including in case of fraud or error, correction mechanisms and penalties in case of infringement to the rules, the intellectual property attached to the technology or the territoriality of the law likely to apply to the network. An agreement between the participants on their remuneration model would also be needed. Furthermore, the governance framework should provide clarity on the entity or group of entities that would be held liable for the activities of the network vis-à-vis third parties, in particular local regulators and customers. ▪ **Privacy management**. As currently designed all the distributed ledger networks (e.g. Bitcoin, Ripple, Ethereum, etc.) and their derivatives are fully open whereby any person/entity with an access to the network can see all account balances and the transactional behaviour of all participants. This is true for both the publicly available versions of these networks and for the private forks of the same networks that financial institutions may choose to run among themselves.

		Banks' customers (and the banks themselves) require their financial data to be private. The lack of privacy poses a problem whereby one financial institution may be able to monitor the transaction flows of another institution perhaps to gain some competitive advantage. One possible solution to the privacy problem is to use advanced cryptography (e.g. Zero Knowledge Proofs, homomorphic encryption, etc.) to obfuscate all the data in the network in a manner that only the two participants in a transaction can actually see what has occurred. From a financial institution perspective this level of privacy would be highly desirable, but it may not be desired from a regulator's point of view who would be unable to interpret the encrypted data in the network and monitor private transactions for market surveillance and AML reasons. The regulator can be granted special cryptographic key that would allow her to decrypt all (or part) of the transaction data in the network. ▪ **Identity management**. Whether it's for AML, KYC or simply being certain of the person/ entity with whom parties are transacting, the identity of the participants in a distributed network needs to be assured. With Bitcoin, identity does not matter. As long as the person at the other side of the transaction holds the necessary secret key, that is all that is required to engage in a transaction. The same can be said for the transaction validators (miners); who they are and where they are located does not matter. Within the context of the financial industry, however, identity matters. It matters that financial institutions know who their customers are, that the regulators know who the financial institutions are and that the financial institutions know who the transaction validators are, and which ones they should trust. It also matters in which jurisdiction the transaction validators are located. The criteria for admittance to any trusted pool of transaction validators are some of the things that need to be carefully considered by the financial industry. Banks need to be certain of the identities of their customers and of the other banks with which they transact. In a world where simple possession of a secret key can control access to funds, it is imperative to know exactly who controls those keys. Regulators will need to determine some appropriate framework that offers guidance on how identity should be handled at every level of the chain. Technical means to exclude certain transaction validators who are not compliant with certain laws or are exhibiting

		bad behaviour (however that may be defined) are required. The governance frameworks should include the rules to determine this. ▪ **Reversibility**. To correct mistakes and fraud, banks require ways to reverse certain transactions. One of the key features of distributed ledgers is that once a transaction is digitally signed it is irreversible from a technical point of view. In the real world, Financial Institutions with experience have checks and procedures to mitigate risks arising from mistakes, errors, thefts and frauds . When transactions are irreversible, there is a significant risk that funds that are sent in error or due to theft or fraud may never be recovered. For distributed networks to be useable by financial institutions, the banks and their clients need to have some assurance that they have some recourse in case of mistakes or worse. A regulator might want to offer some guidelines for reversibility to be ensured in the case of error or fraud. There is also the possibility of requiring some kind of freezing mechanism should digital funds end up in the wrong hands. From a technical point-of-view there are some good solutions available (particularly on Ripple-like and Ethereum-like networks), but the mechanism of freezing and what happens to frozen funds from a legal perspective should warrant some regulatory oversight. ▪ **Settlement Finality**. When funds and assets change hands, there is a point at which the transaction is considered legally settled. With distributed ledgers, assets are represented as digital tokens and the ownership of an appropriate secret key gives the key holder the control over those tokens. With Bitcoin, the movement of tokens in a transaction represents settlement of that transaction (i.e. the tokens are effectively digital bearer assets). They key question for financial institutions to answer is whether mere control of digital tokens represents actual ownership of what they represent in the real world or if those tokens are merely representations of some obligation of a real-world counterparty that would at some time in the future have to perform against those obligations, i.e. are the tokens IOU's or are they actually digital assets? This question is most important when it comes to tokens that represent fiat currency because the problem arises that a token issued by one financial institution may not be valued the same as a token

		issued by another financial institution (i.e. EUR.bank1 may not be valued 1:1 against EUR.bank2). In other words, the differing values of the same currency IOU's from differing issuers may become a problem. In the first case (tokenized asset) much legal and regulatory work should be done regarding the nature of those tokens and to homogeneise the interpretation across the EU. In the second case (differing values of the same-currency IOU's or 'settlement coin'), one solution is to propose that a central bank directly issues digital tokens (either to banks or to consumers) that represent its own currency and for those tokens to be treated in much the same way as cash is today. There are many additional benefits to this approach including fine grained control over monetary policy. Other solutions include the issuance of private settlement coins but that are fully asset-backed by cash at the correspondent central bank. **Technological needs** ▪ **Scalability**. Technology is not scalable at this point, especially when talking about permissionless schemes based on proof-of-work consensus (like bitcoin). Under these circumstances, it is difficult to build practical use cases for financial services. Nevertheless, entry of big technological/ Internet firms (IBM, Microsoft, Amazon, etc.) into the field will help to solve this issue. And in the case of permissioned schemes, scalability probably will not be an issue at all. ▪ **Interoperability**. As DLT will probably be used firstly in niche applications, they would need to interoperate with existing infrastructures. Also, there will be different ledgers for different asset types (or even industries) that will need to interact with one another. Interoperability will also become crucial in the case of several existsting ledgers where two parallel (e.g. intentionally malicious) transactions with the same asset could potentially be executed. A question in this case relates to which transaction has to be considered valid/ legal. There are technical challenges that can only be relieved by the adoption of common standards by all the players in the field. ▪ **Data standards and governance**. DLT and smart contracts need to be underpinned by some level of data standardisation and governance in relation to the formation and maintenance of such standards. This will help reduce complexity and support

		scalability, particularly given the need for interoperability with existing infrastrutures and also to provide a common underpinning for the mulitude of DLT soultions and smart contracts. ▪ **Choice of concensus and cryptology.** Permissionless DLT, such as bitcoin or Ethereum, implement a consensus and cryptology mechanism with a sufficient track record to prove that they work. Permissioned DLT, which banks are more likely to implement, will require different consensus, cryptopolgy mechanisms and ways to retrict access to authorised participants. Those technologies are currently being researched. Therefore data to assess their efficiency and effectiveness is still limited. This is particularly true for cryptology implementation that will require time to be properly assessed. Guidance on the choice of the DLT, its consensus and its cryptology elements, should be considered as important challenges.
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?	The EBF shares the view of ESMA in that they are no major impediments in the EU regulatory framework that would prevent the emergence of DLT in the short term. We also fully support 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 as well as the potential regulatory obstacles. Having said this, as policymakers continue to consider DLT within the context of the regulatory and supervisory framework the following should be considered: ▪ The potential uses for DLT are numerous and diverse. Consequently, the adoption of a "**one size fits all" regulatory framework for DLT is unlikely to be effective**. ▪ If a situation arises where the use of DLT poses challenges within a certain regulation, **policymakers should take a pragmatic approach** to such situations. The possibility of DLT not fitting within certain regulations should not be viewed negatively, given that the current regulatory framework did not envisage a technology like DLT. ▪ **Regulate the specific application, not DLT**: while there may be aspects of the regulatory framework relevant to DLT as a technology platform, this is distinct from applying a regulatory framework to regulated financial activity that uses DLT.

		▪ **Divergent regulatory approaches to DLT in different jurisdictions may hinder the adoption of DLT in an optimally beneficial way.** To this extent, we would urge regulatory cooperation and international harmonisation to enable an effective and facilitative DLT framework. Furthermore we also share ESMA's opinion that a number of concepts or principles, e.g., the legal certainty attached to DLT records or settlement finality, may require clarification. As ESMA correctly realizes, beyond pure financial regulation, broader legal issues, such as corporate law, contract law, insolvency law or competition law, may impact on the deployment of DLT. In particular, the EBF believes that with further development of the technology, the following regulatory issues might need to be addressed by regulators: ▪ Regarding the legal nature of blockchains and distributed ledgers in general, including territoriality (jurisdiction issues and applicable law) and liability (responsibility when something goes wrong) ▪ For the recognition of blockchains as immutable, tamper-proof sources of truth regarding the information stored on it. Related to this, legal framework for the use of blockchains as single sources of trusted identity as well. Harmonized regulation about data protection and definition of identity in the case of legal persons will be needed as a previous step. ▪ For the legal validity of documents stored in the blockchain as a proof of possession or existence. ▪ For the legal validity of financial instruments issued on the blockchain. ▪ For smart contracts in general, settlement finality and in international commerce in particular, including real-world enforceability, territoriality and liability. ▪ For the treatment of shared information in blockchains from the perspective of cross-border flow of data, and data protection in general. Clarification on whether encrypted data is considered personal data is needed. Portability of personal data from one processing place to another.

		▪ Regarding the use of the blockchain as a valid ruling register for the Internet of Things (IoT) ▪ Regulation on how the right to erasure ("right to be forgotten") shall be interpreted, because the tamper-proof feature of the blockchain conflicts with the right to erasure recognised by European regulation on personal data protection. ▪ Legal framework about the legal validity of documents stored in the blockchain as a proof of possession or existence. ▪ Legal framework about the legal validity of financial instruments issued on the blockchain. ▪ The definiton from the regulatory reporting information standards on the DLT. Guidance on which regulator has an access to what type of data stored on the ledger and in which situation. Clarifications on who should run the permission based DLT in the financial sector and who should controls the access rights to the network, (e.g. a supra-national organization on a non-profit basis).
Outsourcing and other solutions with the 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? **(Yes/No/Don't Know- not relevant)** Please elaborate on your reply to whether the current regulatory and supervisory framework governing outsourcing is an obstacle to taking	**YES** The current regulatory and supervisory framework on outsourcing is not updated nor adapted to cloud technology. In the meantime, the EBA launched a public consultation on guidance for the use of cloud computing by financial institutions. It will also update already existing EBA outsourcing guidance that dates back from 2006 taking into account the feedback received from stakeholders to the public consultation on cloud and the recommendations on the matter. There is a need to update the framework on outsourcing, so that it is adapted to the cloud computing technology. Otherwise, there would be an obstacle to the taking of full advantage of the benefits derived from the use of cloud. Current regulatory and supervisory framework is an obstacle to taking full advantage of cloud computing technology. Regulation imposes a burdensome process for financial outsourcing approval and there is a need to bring efficiency to this process.

	full advantage of any such opportunities.	Transfer within the EU is luckily not subject to stricter transferring rules; however security may be a problem in this context. Appropriate safeguards are always necessary.
2.11	Are the existing outsourcing requirements in financial services legislation sufficient? **(Yes/No/Don't Know- not relevant)** Please elaborate on your reply to whether the existing outsourcing requirements in financial services legislation are sufficient, precising who is responsible for the activity of external providers and how are they supervised. Please specify, in which areas further action is needed and what such action should be.	**NO** The current regulatory and supervisory framework governing outsourcing is out of date and too prescriptive. It appears to have been prepared on the assumption that firms would outsource activities completely, on an end-to-end basis. However, firms often use technology solutions as "building blocks" to create larger solutions. Some of the building blocks may be retained within the firm and others provided by third parties. The current regulatory and supervisory framework needs to be amended to give firms more flexibility in how they manage the risks associated with using external service providers On the other hand, there are certain overlaps between the DPA and the ECB/EBA regarding data processing and data protection measures to be taken. If banks do comply with the GDPR and data protection authorities requirements, ECB/EBA should not be questioning how banks are handling personal data that is outsourced.
Other technologies that may increase efficiency for the industry		
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?	▪ Generally, digitalization diminishes paper-based communications, and permits customers to execute transactions/open up services independently of time and place and, if so wished, without need to meet bank staff in person. Mobile banking evolves rapidly. It also allows banks to operate from front to end process. ▪ Distributed Ledgers (i.e Blockchain and Artificial Intelligence) can provide a lot of use cases bringing benefits for financial service providers (and potentially for a number of other industries). Currently the most tested use cases are relevant to Capital markets, Trade Services, Digital Identity/KYC and cross-border payments. Furthermore, most of the initiatives that are being launched in the DLT world have focused on operational cost reduction: syndicated loans management, validation of coverages and guarantees, cross-border payments, regulatory reporting, post-trading processes, identity management (KYC data sharing), etc.

		▪ Robot Process Automation could also reduce operating costs ▪ Big Data can improve risk management and customer experience, bringing agility to financial institutions, while reducing operational costs and improving efficiency. Big data solutions also have a positive impact on IT operational efficiency with a better use of IT resources. To maintain efficient and cost-effective operations, financial institutions will have to be able to manage appropriately not only an explosion of data but also new types and sources of data. ▪ Another example is the use of behavioral biometric as an n-factor authentication to decrease risk and increase security. Behavioral biometric allows the measurement of uniquely identifying and measuring patterns in human activities, for keystroke dynamics, voice recognition or human heartbeats which are unique to everyone. Other examples can be seen in Software as a Service (SaaS) or any type of software automatization in the financial service along with the usage of Artificial Intelligence (AI) such as Deep Learning, open source solutions or the increase of data flow between financial companies via secure APIs. These technologies permit small companies to use new state-of-the-art technologies which are affordable and easy to use, helping them to compete on equal terms with big companies. This process of democratisation in the future will bring new technologies such as Quantum computing or a larger set of IoT capable of detecting behavioral patterns and personalizing services and goods for society at large, reducing cost and increasing efficiency. However, we must bear in mind that these new technologies will also bring challenges such as security and privacy risks for all stakeholders. Accountability and compliance of standards and regulations will be needed to assure mitigation of these risks. Finally, the financial industry compliance obligations (i.e. KYC, AML, etc.) could be more efficient if there were a regulatory framework that allowed public/private institutions (indistinctly) to provide services related to KYC. This framework should include rules, data standards, and control & auditing systems. This type of service will allow the reduction of red tape for necessary duties like due diligences and ensure that technologies and

		providers meet all legal requirements. With this in mind, technologies already mentioned in this consultation, such as big data or cloud, could help to improve processes.
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?	Banks and FinTech Start-ups/non-banking FinTech are seeking to test out new technologies, solutions and business models but are constrained by the existing regulatory framework which does not allow low-risk and low-scale experimentation to take place under less stringent rules. This issue limits competition and may stifle innovation in financial services. Regulators could help by exploring how to gear up in order to support innovation across its activities, working with industry and wider stakeholders. The authorities must provide FinTech start-ups and banks which innovate with leaner and faster authorisation processes. At the same time, we also need to tackle the perception of regulation. Established organisations may be less willing to pioneer new technology due to risk of regulatory censure, whereas smaller firms are perceived to be less at risk. A first step on this journey is to consider the creation of an EU framework for experimentation as a safe space where regulated and non-regulated actors can test innovations in a controlled environment (e.g. sandboxes). It will provide a safe place for firms, in particular to test whether their new products are complying with certain requirements and the legislative environment is adapted to the digital reality. Furthermore, supervisors can pilot the overall digital transformation avoiding market distortions and ensuring the level playing field . The analysis of the impact should be eased significantly and allows supervisors to continuously assess the safety and robustness of the financial services ecosystem. This regulatory framework for experimentation will allow the regulators to assess new products at an earlier phase and potentially amend legislation, when beneficial to consumers, rapidly. This said, it is important to keep in mind that competition law sometimes challenges collective innovation. For example BankID in Norway was collectively delivered by banks, but there is a perception that collective delivery will not align with competition requirements. As a result, this is not leveraged, despite that fact that this would often deliver a better and quicker solution for the industry.

		Examples of 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: **Amendment to the Capital requirement Regulation (CRR):** Amendment to the CRR: "Article 4 Definitions: (115) "intangible assets" has the same meaning as under the applicable accounting framework and includes goodwill, **with the exception of software** for the purpose of Article 36 b)". The banking industry faces the digital challenges in competition with emerging technological players who do not have to face the heavy regulatory burden imposed on the banking sector and are free of prudential regulation altogether. The current regulatory capital framework for credit institutions does not recognize the value of software for capital purposes. The fact that every euro that an EU bank invests in an IT development needs to be backed with one euro of the most expensive category of funding is perceived as a significant disincentive for investments in innovation and a major factor of unfair competition. FinTech companies are not only a major competitor but also partners for European banking sector. However, when a bank acquires a FinTech, its main asset, the software, is automatically depreciated given the deductibility that has to be applied to calculating capital levels for banks. If the buyer would be a non-bank, the deductibility would not take effect. This is like assigning a zero value to the search engine of Google if this were bought by a bank. Because of this, banks may be less open to financing these companies. The regulatory approach to software by the European regulators already acknowledges, to a certain extent, the fact that software has the capacity to generate value, when it comes to the treatment of software for solvency purposes for the insurance industry. Under the solvency framework for the European insurance industry, intangible assets can be recognized for capital purposes as long as it can be demonstrated that there is a value for the same or similar assets. We believe the investments in software should carry the same economic and financial rationale, regardless of the industry.

		Whilst this may not be sufficient, it sets the basis for the solution to the issue in the banking field. Evidence clearly indicates that software has value even in the case of liquidation of a bank. Software has become a core asset for the banks' business models around the world. However, there is evidence of different regulatory treatment of software in some jurisdictions, including the US where capitalized computer software can be recorded as an "other asset" and subject to regular risk rating and not deducted, thereby removing any artificial hurdle to banks investing in digital, creating value for the economy as a whole and for leading worldwide innovation in the area. Furthermore, the European Commission issued decisions on equivalence of the regulatory regimes of third countries to those applied in the EU. Capital regimes of third countries that do not require capital deduction for software has not been considered as an element of relevant discrepancy or inconsistency for the European Commission, neither for the Basel Committee under its Regulatory Consistency Assessment Programme. It led us to believe that the non-deductibility of software does not raise an issue.
3.2.1	What is the most efficient path for FinTech innovation and uptake in the EU?	More active involvement could be beneficial for educational purposes (especially for FinTech start-ups seeking partnerships with banks or other financial institutions), which in turn will help foster an effective environment for innovation. First, it is important to mention that financial innovations help to improve the quality and variety of banking services, complete the market and improve allocative efficiency. As a result, given its gains it is necessary to create a framework that enables their generation. However, it is important to note that the innovation lifecycle is a process with a high degree of uncertainty that comes from several fronts: new uses of technologies, regulatory supervisors' and organisations' lack of experience, new potential risks or unknown legal requirements, just to name a few. Regarding the latter, it is of paramount importance that authorities enable tools to reduce the regulatory ambiguity by establishing collaboration channels with the industry. 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 manage more effectively the new types of issues that might arise in the most efficient manner possible while preserving financial stability and ensuring customer protection. Finally, to ensure a level playing field for all players, all the participants of this ecosystem must observe the principles of technological neutrality, and the same activity should be subject to the same regulation taking into account risk proportionality principles. Regulators have different means to encourage this ecosystem, through tangible means, like tax reductions or by intangible means, like enabling a dialogue with authorities, regulatory sandboxes, one-stop-shops, sharing knowledge. If regulators intend to support new providers, they should do so by supporting the infrastructure and the creation of hubs. These are measures that should be applied on case by case basis, the effects of which can be monitored frequently and adapted as technology and needs evolve. However, if the option chosen to support their growth is regulatory, defining an unbalanced space where traditional banks provide the infrastructure and ensure all the security and customer protection, it will be more difficult to adapt it, whether this framework is used by giants that currently do not need such a support or when new created companies become bigger. ▪ The FinTech ecosystem in the EU is robust and growing with the current level of regulatory engagement ▪ As the FinTech ecosystem continues to evolve, regulators should monitor for emerging risks and take action when required. Nevertheless, authorities must be careful not to over-regulate as this increases the complexity and costs of any new project. In this regard, allowing the test of new technologies within the financial industry is key to understanding its potential effects prior to entering the market, and enabling evidence-based regulations instead of protectionist ones ▪ Authorities shall ensure that there are no undue constraints on collaboration between institutions. Currently there are asymmetries and imbalances between non-banking FinTechs 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.
3.2.2	Is active involvement of regulators and/or supervisors desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants? **(Yes/No/Don't Know- not relevant)** **<u>If Yes</u>**, If active involvement of regulators and/or supervisors is desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants, please explain at what level?	**YES** See response to 3.1. Both approaches are desirable and should coexist, as FinTech solutions can either improve current processes or provide new products and services, as noted in answer 1.1. However, especially from a competition point of view, it is important that authorities leverage the deployment of new solutions with technological neutrality, proportionality and integrity principles, in order to ensure a level playing field among all players. From the point of view of collaboration, it is of paramount importance that regulators allow the testing of new technologies and permit the use of new technologies once their benefits have been proven. These innovations could improve internal tasks related to compliance (like reporting or KYC). An example is the case of the use of cloud services in RegTech solutions, or improved internal processes to reduce costs and improve efficiency, like using DLTs. Although those solutions are focused on improving existing processes, a certain degree of competition among the different providers is expected, so as to foster state-of-the-art solutions. From the point of view of competition, the main contribution should be the deployment of new and better services to customers. This can be done by allowing Regulatory Sandboxes for testing and helping financial providers with one-stop-shops to receive guidance. These new services should not mean a reduction of customer rights or create new risks for the economy. This is the reason why regulators should play an active role before allowing them to enter the market. Finally, as noted above, a level playing field should be guaranteed in order to encourage all players to introduce new solutions to the market.
FinTech has reduced barriers to entry in financial services markets But remaining barriers need to be addressed		

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.	Like banks, FinTech start-ups and non-banking FinTechs should be able to develop services which are available across the EU without incurring costs and slowing down the processes of adaptation of the services to each individual country. We believe that while possible regulatory barriers prohibiting FinTechs and innovation in general to scale up, should be lifted, nevertheless, this should be conducted in a way that adequate security and risk management continues to be ensured, and not at a disproportional burden to credit institutions. As a key example, non-standard transposition of the 4th AML Directive means that a solution developed in one country may not align with the regulations in another member state. In addition, while PSD2 does require a minimum regulatory capital by new players (e.g., that register as a Payment Initiation Service Provider (PISP)), this capital is quite low and possibly does not fully guarantee consumers from the underlying risks involved. Moreover, in case of a customer claim, the Account Servicing Payment Service Provider (ASPSP) (i.e., in the vast majority of cases credit institutions) need to compensate the customer and, only afterwards, seek compensation from the PISP, in case the latter is responsible. One could claim that the abovementioned, while promoting innovation and removing barriers to entry, is not fully neutral between the involved parties. 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. 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. Similarly, not all European countries have developed legislation for alternative finance, creating a mosaic of diverging regulatory frameworks within the EU. In these cases, FinTechs trying to operate cross-border face a practical impossibility due to the lack of passporting facilities. In other cases, practical difficulties to cross-border operations are even more subtle, as in the requirement of certain member states for financial services providers operating

		under passporting to use local IBAN numbers for account holders, which is impossible to achieve by a company established in a different member country.
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? **(Yes/No/Don't Know- not relevant)** **<u>If Yes,</u>** 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** While further detail is required on any proposal from the EC, we would note the following general points on the notion of an 'all-encompassing FinTech licence': ▪ We believe that the EC and other relevant regulators must provide a clear and comprehensive regulatory and supervisory framework before introducing new licensing categories for FinTech activities. - FinTechs activities should have similar, if not the same, capital/liquidity/consumer protection requirements, independent of being offered by a FinTech start-up or incumbents. - The EC must establish a fair and level competitive playing field to address the concern that specially licensed FinTechs activities would be able to offer services and products in direct competition with full-service banks, while being subject to a more limited and less burdensome regulatory regime. - Existing FinTech companies often have atypical funding models and complex equity and ownership structures due to their venture capital and private equity investors, and in many cases will also have non-traditional balance sheet compositions that do not fit readily into the existing capital frameworks for banks. ▪ Discretion should be reserved for activities that are not routine for conventional banks. ▪ When determining what activities are core banking activities, the question to ask is what activities are necessary for a company to undertake to be eligible to be licensed as a national bank. ▪ Related to the issue above, there are financial stability concerns if established tech industry players (Microsoft/Amazon/Apple/Google) and/or merchants are able to seek a limited purpose licence in addition to FinTech start-up (key to this issue is whether non-bank subsidiaries can benefit from the licence). The larger techs/merchants activities would have systemic implications. Any proposal for an EU FinTech licence must have a well-defined scope.

		▪ Issues of consumer protection and financial inclusion must be the subject of consistent, rigorous, and transparent application across FinTech licences and full-service national banks. There are specific activities that do warrant careful attention by regulators, regardless of who is engaging in the activity – namely payments, lending activities, and data storage – as the risks associated with these activities have a far reaching impact to consumers and the broader financial system (i.e. money laundering, terrorist financing, disparate impact, fraud, identity theft, unauthorized transfers, etc.). The types of services offered by non-banking providers should be covered by new types of licences, but if the services are comparable to banking services, they should be regulated in the same way. The guiding principle shall always be "same activities, same services, same risks, same rules". The ESAs should have a prominent role in supervising new entrants (in the same way as they act today in regards to financial institutions) and keepg an EU-wide register of FinTech start-up companies (collecting each national registry) that should be available real time, 24/7 on a pan-European basis. Narrow licences could be issued for specific categories as long as a level playing field is ensured. Passporting is arguably one of the greatest innovations introduced by the EC in its aim to integrate the internal market, and should be available for all regulated activities in financial services. These licences should be activity and risk specific (and should comprise current banking licences). Activities such as alternative finance or financial services marketplaces (digital platforms) could benefit from a clear EU regulatory framework with passporting facilities. 1. Online investment platforms/social trading and robo-advisory registered and subject to specific requirements; 2. Term deposit marketplaces with level of deposits guaranteed by national/European schemes and contribution to such schemes; 3. 100% online banks, application of cross border requirements; 4. P2P Lending, for instance to an NPL framework (debt crowdfunding); 5. Insurtech customer data applied to pricing policies.

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? **(Yes/No/Don't Know- not relevant)** **<u>If Yes</u>**, If you do 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, please explain in which areas and how should the Commission intervene.	**YES** 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. We believe that larger companies are often regulated based on their size, rather than on the risks they incur. Consequently, European regulations should focus on how best to manage stability, integrity and consumer protection risks, rather than just promoting greater competition at all cost. Supervisors can pilot the overall digital transformation by helping innovative FinTech companies (both new entrants and incumbents) within the process and enabling the speed of launch. The analysis of the impact should be eased significantly and allow supervisors to assess continuously the safety and robustness of the financial services ecosystem. It is important to underline that consumer protection is key. A level playing field has the important purpose of guaranteeing that consumers are not put at risk and that financial stability is kept, irrespective of who the service provider is. The development in the field of FinTech can lead to a series of changes with new players, new solutions and new products / services. However, the changes must not undermine confidence in the European financial sector. In this new environment, it is therefore important to determine responsibility for maintaining high customer protection. Common rules for customer protection and supervision are key elements whereby customers / investors can rely on new solutions, products and services. There are some examples of crowdfunding-activities where a company's bankruptcy created losses and lack of confidence among consumers. It is also important that operational risks and information security be taken into account as the threat picture evolves rapidly. The European banking sector creates efficiency and opportunities which a specific focus on stability and security. Consequently market confidence and the protection of both consumers and investors are fundamental components. Requirements and opportunities should be proportionate and the same for all types of companies, small and large, newly formed and existing companies as soon as they develop similar services or products (so called level playing field). For FinTech activities, it is therefore important to take into account the stability and security of the financial market, including: ▪ High confidence in the banking sector

		▪ Customer protection, consumer and investor protection ▪ Well-functioning and competitive regulations, both nationally and within the EU and internationally ▪ High security and well-functioning infrastructure for payments FinTech initiatives developed by banks, non-banking FinTech and FinTech start-ups should be able to count on this flexibility especially when they are developed by providers who are already operational. In order to achieve proportionality in the cybersecurity strategy, the regulatory framework applied to cyber security and/or cyber risk should be based on internationally recognized standards. The ICT Risk Assessments should be proportionate and based on principles and internationally recognized standards such as ISO and NIST. Also this proportionality should give room to the risk appetite of each FinTech company based on proven evidence that the risk has been properly 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? **(Yes/No/Don't Know- not relevant)** 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** In certain countries, banks have national l law banking secrecy/client confidentiality obligations in addition to general data protection requirements to consider when flowing data both within and out of the EU. Data flows are an integral part of companies' daily trade and operations. Their ability to transfer data throughout the world is vital including for banks, no matter their size or the geographic area in which they operate. One of the main obstacles 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. Frictions to leveraging the benefits of Cloud Computing in Financial Services arise when data regimes restrict cross-border data flows, both within the EU and globally. Data stored in a Cloud Computing environment can be fragmented geographically and its support functions (such as processing, hosting, backup, support and management), divided among suppliers (often across national boundaries) to enhance their data security,

		disaster recovery and resilience. In this regard, this progress in technology towards a 'distributed' network infrastructure challenges traditional data and outsourcing concepts such as the physical data localisation and auditing of physical premises. According to the financial rules on outsourcing for many EU countries, financial institutions must notify the supervisor and obtain their approval to launch cloud projects. This notification and approval has to be done on a case by case basis. It implies an indirect constraint to the free flow of data and, thus, to a faster innovation and a more agile cloud adoption. There is a need to harmonize EU financial supervisors' criteria when approving cloud projects Prescriptive regulations on data localisation are at odds with trends in technology. The latter, unlimited by geographic boundaries scan manage storage and access to data, located globally. We observe that several EU countries have introduced, at national level, additional limitations and barriers which prevent data circulation and intra-group synergies at EU and international level. These have an impact on risk management, centralised/shared infrastructure strategies, and the ability to provide products and services to global customers. Banks need to be able to transfer data across borders efficiently so as to respond to customers' needs: delivering goods and services, processing payments or providing customer support. To achieve cross-border data flows, there must be no direct or indirect restrictions on data localisation. Limiting data flows without objective and justified reasons undermines the ability of companies to define their business models; it will be detrimental to competitiveness and growth of EU companies; and, endanger the functioning of critical infrastructure. Whilst Member States' interests in national security and law enforcement in most cases are fully legitimate (not least those linked to non-personal data), one can argue that there is no valid justification for data localisation. In practice, these interests are too often used to justify, largely unrelated, measures. We agree with the Commission's statement that localisation restrictions rarely advance the public policy objectives they are intended to achieve.

		The EBF fully supports any EU initiative that could remove restrictions to the free flow of data which at the same time acknowledges the right that businesses have to choose where they store their own data. Companies 'decisions on data localisation may be part of a specific business model and companies must be allowed to request or provide data localisation. This is a choice made by both providers and recipients of the service, which is quite different from a legislation obligation to do so.
3.7	Are the three principles of technological neutrality, proportionality and integrity appropriate to guide the regulatory approach to the FinTech activities? **(Yes/No/Don't Know- not relevant)** 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 consider that the three principles are appropriate, but probably not sufficient. Technological neutrality is clearly desirable and facilitates the self-selection of the best technologies by market forces, although it is not sufficient to guarantee a level playing field. Proportionality is needed as a risk-based approach that takes into account specific activity risks, and not whole company risks by default. Integrity and competition are beneficial to all stakeholders, and should always be promoted. Stringent prudential, security, investor and consumer protection regulation is an inherent part of the regulatory framework in which banks have to operate and has been reinforced in recent years. New entrants are less burdened by regulatory requirements and they tend to choose the optimum legal structure to avoid the heavy regulatory burden of the financial sector. Similarly, they are not subject to the same levels of scrutiny from supervisors and authorities. The implications of this for policy objectives concerning consumer/investor protection, fraud and financial crime, and financial stability must be taken into account. Finding a proper balance, and future-proofing it, will be one of the main (and on-going) challenges for policymakers, regulators and supervisors for the years ahead: how to encourage the development of financial technology and to bring dynamism and competition into the financial sector both for incumbents and new entrants without leaving the financial sector open to new risks or significant failures and thereby endangering financial stability, with possible loss of public confidence, or creating an uneven regulatory framework. Customers and investors' trust will be gained if they are confident that the same level of protection is available no matter which entity – banks or non-banks alike – is providing the financial services.

		From a supplier's perspective, the concern is that a loss of trust by consumers in one area of the industry, whether that be a FinTech start-up or a large incumbent, harms the sector as a whole. With equal rights must come equal responsibilities. Cybersecurity is a good example of this principle. A failure by any single market participant harms reputation and damages trusts in the industry as a whole. Policy makers should consider the importance of ensuring that an internationally recognized standard is applied and supervised across all market participants. Regulatory guidance so as to avoid the "reinvention of the wheel" should be provided to avoid ending up with many different standards and further fragmentation. In a nutshell, the concept of "same services, same rules, same risk, same supervision". Technology (and digital platforms) neutrality and cooperation are also important concepts in this respect, as otherwise banks will face competitive disadvantages from certain competitors that control digital platforms on which banks and many other businesses also fully depend to offer their digital services. The Digital Single Market is an opportunity for all operators willing to embrace the digital transformation: authorities, banks, FinTech start-ups, corporates and consumers. The achievement of their respective digital ambitions calls for a regulatory framework that takes into account two important considerations: 1. Allow for competition to unfold: a number of adjustments to existing legislation / regulatory frameworks and right-sizing of regulatory requirements need urgent attention for competition and a Digital Single Market for financial services to take off, and must be addressed in the short term. Put Digital first: a thorough fitness check by the EU of the existing complex regulatory framework is necessary to ensure it is fit for purpose to support banking in the digital age. To be clear we see no need to create new regulation for the digital era but consider it important to make a thorough and comprehensive review of existing legislation to ensure the current framework is up to date, future-proof and does not impede innovation and competitiveness in the Digital Single Market for financial services. Furthermore, regulation must not unduly constrain banks or FinTech start-ups from providing an effective response to the challenges posed by digitalisation. In this context, it should be underlined that technology is moving faster than changing regulation. If the regulation is principles based then the innovation can continue

		without waiting for the legislation to catch up. For example, there have been issues in the UK with people having all their utilities digitally managed, with no paper proof of address documents which banks want require for opening an account. Yet, government approved guidance was that paper documents should be taken rather than digital copies. Had the guidance been principles based the issues with access could have been avoided. 2. Promote innovation and avoid unintended disincentives: regulation can also be observed as a disincentive to experimentation. Undertaking regulated activities in various Member States usually requires explicit permission from the regulator and approval of the way in which the firm in question goes about its business. A risk-averse regulator may not be willing to grant permission to unfamiliar or unproven business models. Unregulated entities may, however, find it easier to undertake new business without having to comply directly with the regulator's tests. Similarly, digital services can easily cross borders, and varying risk appetite among regulators and overseers may hamper the cross-border provision of services and unintendedly lead to market distortion.
Role of supervisors: enabling innovation		

3.8.1	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?	The EBF supports the development of a framework of experimentation/testing framework ("EU regulatory sandbox") which implies a combination of both national and EU framework as best option. Currently we observe that supervisory authorities have a diverging approach on this issue, leading in certain cases to a huge competition among the supervisory authorities to attract innovative companies to their countries. In our opinion the following steps should be considered with a view in the long term to achieving an EU regulatory framework of experimentation: 1. First, a collaboration among EU and national institutions should be considered, as each of them has different legal powers, goals and, even jurisdictions. The creation of an innovation friendly environment might require an interaction among the authorities. 2. A coordination should be conducted by the European Supervisory Authorities and promoted by the European Commission with the monitoring of good practices and the elaboration of guidelines or high-level principles to ensure a consistency in the approach and help companies to innovate faster without being confronted with barriers at national level. It will guarantee that all different national initiatives have a coherent approach, allow similar exceptions across the EU to avoid any uneven level playing field between different Member States. 3. It should lead in the long term to the establishment of an EU framework of experimentation, open to all innovators, and with a participation on a voluntary basis. The aim of such framework of experimentation should be to : ▪ Represent a 'safe spaces' in which businesses can test innovative products, services, business models and delivery mechanisms without immediately incurring the normal regulatory burden of engaging in the activity in question; but it should not be understood as a shortcut to avoid legal requirements at national or EU level . ▪ Facilitate a dialogue between banks, non-bank FinTechs/FinTech start-ups and regulators on the regulatory barriers to partnerships or to the deployment of innovative services/technologies.

		▪ Ensure a level playing field: among all innovative companies and among the supervisory authorities to favour the deployment of innovative solutions in the EU and avoid any fragmentation between Member States; ▪ Bring clarity on the applicable rules /Education with guidance on the interpretation of the legislation in relation to the testing activities; ▪ Facilitate the collection of new ideas, identification of new innovative services, monitoring trends and addressing the innovation especially in the perspective of potential regulatory adjustments and integrations.
3.8.2	Would there be merits in pooling expertise in the ESAs? **(Yes/No/Don't Know- not relevant)** Please elaborate on your reply to whether there would be merits in pooling expertise in the European Supervisory Authorities.	**YES** The ESAs currently play a limited role in the area of financial technology. While it is important to take advantage of technological developments it is also crucial to address major risks arising in this context. Besides specific initiatives such as the establishment of an "Innovation Academy", the ESAs should seek to make a greater use of the stakeholder groups, which can be very efficient on more complex and technological issues. ▪ One of the key assets for enabling an innovation ecosystem is to improve the learning skills of all stakeholders, improving the empathy of all interested parties and enabling a creative process to achieve a common goal. However, not all participants have the same knowledge at the outset. ▪ As products and services are opened up cross border, so will the risks and challenges move across borders. Sharing of knowledge and experience between ESAs will ensure that national regulators are best placed to learn from each other and deliver guidance of value to their sector to ensure that the overall sector is hostile to financial crime. ▪ Information sharing at this level is optimal for collation of issues that should be resolved through legislative change then fed back into the EU legislation process rather

		than each Member State trying to solve the same problems leading to further disparity in standards across Member States. ▪ Furthermore, it is important for each Member State to listen to the needs, requirements and objectives of the other before taking any decision. In this scenario, it is paramount to ensure that the opinion of experts in each field is achieved. This pool should include all relevant stakeholders: authorities, industry, consumers and academic researchers.
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? **(Yes/No/Don't Know- not relevant)** **<u>If Yes,</u>** if you think the Commission should 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, please specify how these programs should be organised.	**YES** An "Innovation Academy" set up by the European Commission, coordinated by the ESAs and supported by financial (and non-financial) associations and Research & Innovation banking centers, could help train subject matter experts with a common background, able to spread the FinTech's culture of innovation and to promote the development of innovative solutions but might not be sufficient to ensure that relevant competences exists within the relevant DGs of the EU Commission, the ESAs, local NCA and other bodies in order to understand market developments and regulatory challenges better. Legal skills, futurologists, innovation centers, university professors, innovative entrepreneurs could be involved. Deliverables could be useful contents for the Commission, like surveys, trends monitoring, and consumer behavioral change. In our understanding, 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 rejection of certain financial innovation projects; best practice case studies; as well as reports regarding the use of new technologies and forecasting studies. Another important issue is to ensure that all potentially interested parties are represented: the industry, consumers, academic researchers and all competent authorities. Regarding the latter, it is of importance to mention that 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 in this Innovation Academy. To conclude, an effort to identify all required legal stakeholders in all financial fields should be done prior the introduction of this Academy so as to ensure that there is a correct representation. Nevertheless, this framework should include authorities related to the financial industry but also from other fields such as DG Connect or any other technology related authority as FinTech has a strong technological base. These programmes could be organized as suggested below: ▪ **Organization:** the nomination process through local authorities; participating teams, not too large, to ensure exchange and discussion; representation of all interested parties from the authorities, academy, consumer representatives and industry (this can be arranged in different committees to ensure that teams remain focused and not too large). ▪ **Physical meetings** in different EU countries to improve relationship management ▪ **Topics**: current issues from national or EU parties invited; future challenges and how to handle them; insights from experts; knowledge created by the different innovation initiatives which can be rapidly be implemented (i.e. from sandboxes, incubators, etc.) ▪ **Selected topics** ▪ **Method**: use modern, interactive and solution orientated methods and techniques (design-thinking, prototyping, etc.) case studies, rationale applied for the different decisions, etc. In addition, the Commission in the context of the innovation academy could create an awards' programme to reward FinTech initiatives at the national, regional and local level. The objectives of the awards would be to: ▪ identify and recognize successful activities and initiatives undertake ▪ showcase and share examples of best entrepreneurship policies and practices ▪ create a greater awareness of the role FinTech play in society

		Encourage and inspire potential FinTechs activities (from banks, non-banking FinTech/FinTech Start-ups). Finally, the creation of an EU Innovation Academy should not exclude the efforts of the different companies in this field and the participation should not be compulsory. However, we would like to note that one of the main problems for policy makers is the lack of empirical knowledge and the inability to forecast in order to deploy future-proof policies. In this regard, we welcome the creation of an Innovation Academy to fill this gap by organising the knowledge already generated and ensuring it can rapidly be implemented by policy makers and companies.
3.10.1	Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS? **(Yes/No/Don't Know- not relevant)** Please elaborate on your reply to whether guidelines or regulation are needed at the European level to harmonise regulatory sandbox approaches in the MS?	**YES** See response to question 3.8.1
3.10.2	Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border? **(Yes/No/Don't Know- not relevant)** **<u>If Yes</u>,** If you would see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border, who should run the sandbox	**YES** See response to question 3.8.1

	and what should be its main objective?	
3.11	What other measures could the Commission consider to support innovative firms or their supervisors that are not mentioned above?	The aforementioned initiatives focus on the supply side, but there is a lack of initiatives related to the demand side. Thus, the measures that the Commission might consider supporting could be as suggested herewith. ▪ Policies to improve financial/digital literacy for customers to understand the benefits and risks that they assume when using these new services. These policies should be targeted at individuals as well as any company that offers these types of services. As an example, the increasing use of customer data to improve services, aligned with the GDPR. ▪ Authorities must strengthen their supervisory role on the new services that arise, taking a proactive role when the service provider does not meet the legal requirements or exceeds its licence, providing services that have not been authorised. This measure ensures that customers only access safe and secure financial services and avoids misuses that might damage the reputation of all services providers. A register of local irregularities or differences in regulation could be considered. It is a difficult task to identify the relevant level of oversight, regulation and control. If regulation becomes too tough, innovation will suffer. It is probably more relevant for supervisory authorities to have some degree of control and oversight but yet with some leeway.
Role of industry: standards and interoperability		
3.12.1	Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision? **(Yes/No/Don't Know- not relevant)**	**YES** We do not believe that the European System of Financial Supervision (ESFS) needs to play a more proactive role in the development of standards. There are however opportunities to promote global standards in a way that would support the objectives of the European Commission.

	Please elaborate on your reply to whether the development of technical standards and interoperability for FinTech in the EU is sufficiently addressed as part of the European System of Financial Supervision.	We strongly believe that the Commission's approach should continue to look at outcomes, be technologically agnostic, and regulate based on the products and services offered. It is undesirable to apply the generic labelling as 'FinTech' – that the institutions normally use – to supervision or regulatory requirements". We believe that – in line with the objectives of the European Commission and the ESFS – standards are central to systemic risk management and subsequently end-user protection. Standards can work as an enabler to unlock opportunities for new entrants and for enterprise-wide regulatory risk management by bringing together the regulatory framework on an ongoing basis. In the context of the FinTech industry, the European Commission and the ESFS should look at promoting and at recommending the adoption of global standards before considering jurisdiction based standards. We see this benefiting the objectives of the European Commission and the FinTech Industry because FinTech is global in nature and the use of standards to support competition, manage risk and promote interoperability should be considered from a global perspective. By its very nature, FinTech often includes products and services that are not jurisdiction-specific, such as data processing, cross-border payments, settlement reconciliation. As a result, it would almost always be counterproductive to seek to move towards anything other than global standards.
3.12.2	Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities? **(Yes/No/Don't Know- not relevant)** Please elaborate on your reply to whether the current level of data standardisation and interoperability is an obstacle to taking full advantage of outsourcing opportunities.	**NO** The current level of data standardisation and interoperability is already increasing and we believe that there are no specific obstacles for FinTechs here in this field nor in outsourcing. Some countries are more advanced in this but it is a process that should be left to market forces in order to set more appropriate standards for all and ready for development when the technology changes. If there is regulatory action in this field, it should be limited to minimum conditions and be technology neutral. Indeed, as FinTech operations are not always subject to oversight by Financial Authorities, FinTechs are better positioned for outsourcing than incumbent financial institutions. Nevertheless, we agree that standardisation would foster competition and interoperability on the "standardised" activities as long as these standards do not hinder innovation but ensure a level playing field among FinTechs and established Financial Institutions. Thus, interoperability is very positive, provided it is developed in a way that ensures high levels of cybersecurity, data safety and customer protection. We are seeking collaboration with third parties in a win-win scenario in which banks and FinTechs develop customer

		centric products that are both secure, cost effective and innovative. To that effect, a wide adoption of Application Programming Interfaces (APIS) will pave the way for a secure, competitive and innovative environment for financial services as it is already the case today for many other online activities and interactions.
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?	The consultation paper correctly identifies that standards create common understanding and promote interoperability, allowing new products and services to connect and interact with existing and developing financial infrastructure in an efficient and secure manner. In our views, every player should contribute in the same way to these objectives and there should be a balanced allocation of responsibilities. Competition should be promoted and new entrants should be welcomed but not by means of lowering current protection levels consumer enjoy, as this will lead to a less safe market. In the context of FinTechs, the objectives of efficiency and interoperability can only be enabled by standards if they are developed at global level, are outcome based, technology agnostic, transparent, and inclusive. We believe that existing mechanisms (e.g. the ISO governance and procedures for developing and maintaining new and existing standards) provide for this. We also note that the use of global standards could enable other pieces of work that could suit the European Commission's objectives. Not only does the use of global standards remove the need (and cost) of developing new standards, it also minimises the cost, for those already familiar with global (ISO) standards, to minimise lift. For example, we note that the consultation paper looks at the possibility of a role for the European Commission in developing sandboxes. While we note that the term 'sandbox' is generic, it is still possible to argue that standards would play an important role in providing interoperability of sandboxes/framework of experimentations and/or of their participants. Standardising on-boarding processes, semantics, and financial messaging standards are examples that would benefit the use of framework of experimentation across the European Union.
3.14	Should the EU institutions promote an open source model where libraries of open source solutions are available to developers and	**NO** This does not appear to be an appropriate role for EU Institutions but rather depends on the choice of IT developers (or other owners of IP rights) to make their solutions available on an open source basis EU institutions should focus their efforts on supporting and

	innovators to develop new products and services under specific open sources licenses? **(Yes/No/Don't Know- not relevant)** 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.	creating a legal framework that allows open source models to flourish but not promote any particular open source model. The development of libraries of open source models and solutions is indeed so rapid that acceptance by the institutions of spreading standards could slow down the exchange of non-commercial or sensitive information as well as the free choice of the best standards with respect to the needs of each party.
Challenges		
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.	FinTech, considered generally, can improve safety and soundness by reducing errors and making the firm more efficient. For example, Data analytics / Big Data allows us to access and analyse data in ways that we could not have done before. The re-engineering of our Market Risk platform, which now manages over 1 billion risk sensitivities, provides visibility 17 times faster than the previous system while delivering a more granular and holistic view of the firms risk exposure. However, FinTechs also represent an opportunity for incumbents firms to develop new partnerships which can create efficiencies in terms of cost reduction, (e.g. back office processes), better capital allocation and customer acquisition. (For example, on boarding and front-end processes especially with the use of AI, RPA, video communication, biometric data).

		Collaborating with FinTech companies can also generate efficiency and improved services/products, by connecting external ideas with incumbent knowledge, data, space and other resources to co-create innovative solutions Moreover we expect quite a big impact by the FinTech on incumbent firms (Third Party Providers – TPPs) due to the new regulatory framework (eg. PSD2, GDPR) and the competitive arena they introduce. There is however a risk that retail financial services become spread across many suppliers: it will become challenging for any supplier to identify suspicious activity as no single supplier will have an holistic view of the customer. Consequently, a secure, harmonized and reliable environment is of paramount importance to allow market participants to identify themselves in a standardised manner, to provide a secure access to payment accounts where customer consent is collected and respected at all times (access to sensitive financial data or not). PSD2, together with the GDPR, the EBA draft final RTS and the ERPB Working Group all contribute to building this environment that is welcomed by most FinTechs and should not be undermined by a short term political agenda. In that way, one can preserve the right balance between competition, innovation, security and consumer protection. Each player should bear its responsibilities in terms of customer protection, financial stability and cybersecurity, failing which we risk putting the security burden on banks only, by that affecting the stability and security of the entire payment ecosystem.
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	The free flow of data should be significant, in order to develop the Digital Single Market for financial services. Data is growing exponentially, in terms of use, variety, volume and velocity. Data is at the centre of the digital revolution and consequently data analytics is increasingly creating new opportunities both for consumers, who can benefit from more innovative and tailored products and services adapted to their needs, and for companies able to develop new

	when their data is processed by service providers for commercial purposes that go beyond their direct relationship?	innovative businesses. A number of challenges though, remain, arising from the misuse of data, information asymmetries and data security. Such concerns are taken seriously by the banking industry, as trust and integrity are its biggest assets. Confidence in banks as trusted parties is essential for their reputation and business model, a fact which adds to the effort and investments put into maintaining and improving setups, guaranteeing the safety of customer data. The benefits of digitalisation can only be reaped if each and every stakeholder follows the same rules, and if the financial services' industry can apply data-based innovation in a clear regulatory environment that is the same for all players. 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. 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. If we agree that data is the most valuable asset in the digital world, helping European players to deploy the highest capabilities in data is essential in order to guarantee their competitiveness. The success of the Digital Single Market inevitably depends on it. As a result, 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 the privacy rights for consumers. Further consideration should also be given to enhancing the cooperation between the competent authorities regarding cybersecurity, data sharing, or to ensuring further legal certainty in the interpretation of the General Data Protection Regulation (GDPR). Data issues constitute a key commercial and strategic business decision for a company. Data have a strategic value for entities and this value is fundamental to being able to compete fairly in Digital Markets and in the Data Economy.

		It is not clear, at this stage, that banks would have a commercial or financial interest in trading non-personal data. In our view, the intention of the European Commission to address the issue in contracts (data usage licences) is a good option. Guidance on how to avoid misuse of data would be welcome. Importantly, the sharing of non-personal data with other operators for the banking sector needs to be voluntary and according to a price or a negotiating contract. According to their business strategy/model, companies need to be able to leverage the data value in the market and, furthermore, be able to protect and avoid sharing the data that they want to keep safe, or which is only for internal proposes. Besides the costs and value of data, there are opportunity costs and risks (i.e. regulatory compliance) and cyber risk issues to be considered. As such, we believe non-personal data owned by financial companies may be shared against payment but always on a voluntary basis. We should also take into account the different kind of data, bearing in mind that enhanced data are part of an organization's know-how, which means that they should be the ones achieving the benefit given their invested resources and intelligence to enhance raw data. Consent is very important when using a person's data in this manner. It is important to establish that compensation should be agreed between the two parties. It is also important to keep in mind that a fair compensation should not necessarily be understood as a payment to the user or as a direct economic compensation for allowing data processing. The benefit is often derived from the user having access to a more personalised, global and tailor-made service or having certain service/products benefits in exchange.
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?	The financial services' industry already has a range of tried and tested solutions for storing and sharing financial information. New technology and process are constantly reviewed to assess whether they can generate efficiency or improve services. The Distributed Ledger Technology (DLT) is no exception and the financial industry has been investigating the potential merits of this technology for several years. It is not a panacea, but there are some specific use cases where DLT might offer reliable solutions.

		So far many of the **most useful solutions have appeared in the post-trading environment**, however, over time we expect to see other solutions making use of DLT technology. For example, 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 (even when signed off the ledger) are some of the types of information that could be stored in a Distributed Ledger. The EBF believes **DLT might be complementary to APIs**. DLT is generally better for pushing or broadcasting data, APIs are good for pulling data. DLT by itself is not suited as an information store, but it might be optimal for data synchronisation between multiple organisations. DLT solutions are actually more reliable tools than other solutions for storing and sharing any kind of information if they are well designed, because they are decentralized, so there is not a single copy of data to be attacked, and every copy of data is synchronized so every node in the network is seeing the same information. However, reliability depends on a solid design of the solution, including security, governance and privacy issues. Participant nodes in the network have to be properly managed and subject to very strict rules regarding cybersecurity measures, cryptographic key management and encryption mechanisms put in place. Liabilities of these participants have to be clearly defined in case of a data breach. Also, a clear definition of which "slices" of information can be accessed by each and every node in the network is essential. Of course, there are alternative technological solutions available for storing and sharing financial information. There are many other architecture models that can achieve the same purpose (i.e. APIs/ microservices/SOA/PKIs, etc). Additionally, shared databases have been used for years, but they lack some positive built-in capabilities of DLT solutions: immutability, decentralized administration, multiple synchronized copies, etc. These capabilities could probably be replicated by adding functionality layers to shared databases but they will result in more complex infrastructures.

4.3	Are digital identity frameworks sufficiently developed to be used with DLT or other technological solutions in financial services? **(Yes/No/Don't Know- not relevant)** Please elaborate on your reply to whether digital identity frameworks are sufficiently developed to be used with DLT or other technological solutions in financial services.	**NO** Digital identity is arguably one of the most important aspects to successful DLT adoption. In a distributed network environment Digital Identity is of paramount importance to ensure trust. Without trust, DLT implementations will fail. However digital identity frameworks are currently not sufficiently developed and even if they were, regulatory fragmentation across Europe regarding digital identity remains a big obstacle for a harmonized European digital identity framework as eIDAS could be. DLT meets the strong regulatory requirements for customer identity proofing and verification for Know-Your-Customer and it also complies with the legal certainty and validity of qualified eSignatures established by eIDAS regulation that will enhance the security of electronic transactions. But it is also necessary to harmonize the European framework regarding the prevention of money laundering and terrorism financing (AML/CFT), to ensure the 4th Anti-Money Laundering Directive is implemented in a consistent way as the acceptance of the means for identifying customers remains with the Member States. Once that framework is set, the use of DLT can help to store and share digital identities between financial services players, facilitating KYC processes. It should be noted that for certain DLT uses cases, digital identity frameworks, considered at the individual / end-investor level, will not be an obstacle. For example, for DLT applications with institutional participants as nodes, which will likely use a more typical account structure and permission-giving approach to manage client "identity."
4.4	What are the challenges for using DLT with regard to personal data protection and how could they be overcome?	Data held within DLT is very likely to be encrypted. However, with continuous increases in computing power and technological advances, we assume that any encryption applied today will be compromised in the future, maybe in 3 years, maybe 20 years. Consequently, we would treat DLT 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 see the data, regardless of encryption. For DLT this leads to two scenarios that can be applied to data sharing: ▪ the DLT does not hold personal data, but may hold pointers to where the data is held. ▪ the DLT supports scenarios where the data elements are only shared with a specified subset of network participants, not all participants. There are various forms of DLT solutions, including solutions where the data is accessible only to users who have been given appropriate access. The existing legal and regulatory

		framework provides sufficient protection. To introduce regulatory requirements specifically for DTL solutions would be contrary to the Commission's stated objective of being technology neutral. Restrictions on transfer of data across national borders potentially creates a challenge for use of DLT solutions. However, the same applies to other technology solutions, e.g. cloud computing solutions. Additionally, it is important to underline that DLT implies high quality data, being consistent, complete and accurate. However, currently there is no harmonized regulation on data protection on a global scale. 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. The General Data Protection Regulation (GDPR) introduces a new right to erasure or to be forgotten, implying that, under certain circumstances, individuals have the right to obtain the erasure of their personal data. This new right introduces a debate as to whether and how the right to be forgotten can be compatible with the immutability of the blockchain. The DLT does not necessarily threaten data protection. On the contrary, it can 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. On the other hand, solutions like private or permissioned blockchains and strong encryption can be considered. In the future, the widespread adoption of blockchain might remove the need for large companies to maintain data and provide individuals with complete control over their personal data.
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?	Historically, SME risk has been hard to profile in some countries. Technology besides increasing the amount of information available, reduces data errors, duplications and differences. It should also be underlined that, in recent years, non-bank funding providers' lack of view on SMEs financial background has been offset by higher commissions, something intrinsic to higher risk taken by FinTech star-ups in comparison to traditional banks.

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?	Data protection and customer confidentiality requirements restrict banks and other financial services firms from sharing information on their customers with third parties, whether SMEs or other categories of customers. The market is already very open and does not require any additional provision until regulations such as PSD2 and GDPR 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 more affected by initiatives to open data, in relation to the rest of the sectors that do not have similar measures (and whose data is also relevant for the provision of credit). 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. Market mechanisms (such as the freedom to decide on a fair price) could also lead to more counterparties being willing to provide data to alternative funding providers, especially given the increase in the number of players that are now collecting and processing data, and thus augmenting the data offer. 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.
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?	It should be noted that the key issues underlining the following answers are the creation of a level-playing field and the safeguarding of consumer (including data) protection and financial stability. We do not see a need for additional requirements but we do see a need to extend/update the existing ones so as to include all players besides banks. The Directive on security of network and information systems (the NIS Directive), GDPR and PSD2 have created a new regulatory framework for cybersecurity in the UE but are still being implemented. On that note, new regulations such as PSD2 or the NIS Directive are centralizing the risk on specific elements in the security chain such as banks, CSP or critical services, but are

		not considering other players that may be weaker or more vulnerable in the chain, thus incentivizing cybercriminal cyberattacks on the weakest, or easiest to attack. There is a need to harmonize these regulations so as to demand the same risk-based responsibilities. Moreover, the development of data dissemination leads to greater risks. In this case the responsibility of each player should be clearly defined and borne by each in the event of an incident. It would be desirable to have a traceability standard applying to all players to be implemented very quickly in order to maintain effective fraud detection systems. Regulatory obligations, particularly in terms of actions needed on cyber security, should be extended to all players who handle financial data and operations. In addition, it is not only about expanding requirements to other players but also about ensuring that those players are properly supervised. In general, regarding any regulatory approach to cybersecurity, we would stress that effective cyber defence requires a global perspective. These efforts require constant collaboration and strong partnerships to counter innovative threat actors and evolving risks. As such, financial firms must collaborate with government partners around the world, other financial industry partners, as well as vendors and clients to address cyber threats effectively. We strongly support regulatory harmonization by global supervisors around risk-based approaches to cybersecurity risk management. The G7 "Fundamental Elements of Cybersecurity for the Financial Sector" provide a starting point for all cybersecurity regulation. We consider the NIST framework to be an example of an instantiation of the principles defined in the G7 "Elements". Regulatory efforts should focus on the simplification of the current regulatory framework, creating a one-stop-shop mechanism for incident reporting regardless of the regulation setting the obligation and harmonizing incident reports and taxonomies. The increase of services available online can lead to an increasing number of attacks to the financial sector. However stricter ICT risk requirements should not create prescriptive obligations, but leave a margin for the banking industry to apply risk based approaches. Cybersecurity requirements should be proportional to take into account the size and complexity of the

		company, but for smaller companies they should not be lowered to the point where they do not ensure an adequate level of protection. The following approach should be considered. ▪ It is necessary to set a common EU cyber-security framework to assess and manage cyber security/risks. We are aware that EU bodies are applying in certain on-site reviews the (US) NIST Cyber Security Framework. ▪ It is necessary to define a common EU methodology and common EU criteria applicable to (cyber) incident reporting to different EU bodies (for example, to SSM cyber incident reporting, PSD2 incident reporting, GDPR incident reporting, Critical Infrastructure cyber incident reporting). ▪ It is necessary to set up in the EU a global body empowered to produce timely reports on the most relevant cybersecurity threats suffered in EU countries. At present, information on this is drawn mainly from US sources. If provided with the required resources, we think that ENISA could play this role. ▪ It is necessary to entrust to an EU body the definition of a common pan-European methodology and criteria to certify cybersecurity providers and foster the emergence of certification providers according to this methodology. This should apply to players other than those covered currently by the NIS Directive (FinTechs, hardware/software vendors, etc.). ▪ In the case of IT outsourcing done by financial entities, key services providers have to be audited and certified for cybersecurity by each of the financial entities with which they work. In order to make this procedure efficient and it results consistent, it is necessary to define a common methodology and criteria to perform this kind of audit. ▪ Market infrastructures concentrate risk and FinTechs may play a role in de-risking them, for example, through the use of DLT solutions. It is highly recommended to provide specific technical standards, such as the NIST frameworks. This way all financial institutions / FinTechs will self-regulate themselves based on predefined technical standards. EU can provide a framework with which everyone should comply, and provide strict and specific configurations (e.g. a set of approved cryptographic algorithms). In addition, existence of an international standard (e.g. ISO) as an EU prerequisite for the operation of such providers, would further strengthen confidence to and security of the related services.

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?	The banking industry for the purposes of own resilience and risk mitigation needs a legal framework which allows financial institutions to share among themselves sensitive information related to fraud & cyber-attacks at national and cross-border level. For this purpose, the banking industry would call upon an active dialogue between the industry, the Article 29 Working Party (EU Data Protection Board), the European Banking Authority (EBA) and the European Central Bank in the context of the Single Supervision Mechanism (SSM) with a view to assessing how best to enable this sharing of relevant (including possibly sensitive) information.. This said, firms often collaborate with other members of the financial industry beyond interaction with governments and regulators. The belief that cybersecurity is not a competitive issue has allowed the industry to work together to improve the cyber defences of the sector as a whole. Information sharing and coordinated analytic work have been the hallmarks of sector collaboration. Technical frameworks and solutions already exist in order to share threat intelligence information or other threat/risk data. An EU Banking CERT/CIRT could regulate the rules of sharing such information. The sharing portal for threat intelligence information could serve as an early warning input for imminent threats. In our opinion, the following act as hurdles which 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 authority will translate into demands on providers to report the same type of incidents to different regulators, which will increase the burden for all companies regardless of their size. It is necessary to harmonize these demands and establish a one-stop-shop mechanism for incident reporting to all relevant authorities and regulators in relation to different legislative pieces, such as the PSD2, the Network Information Security directive, the General Data Protection Regulation, eIDAS regulation, etc. Reporting procedures, templates and methodologies used in the different Member States should be streamlined and made consistent.

		▪ National Competent Authorities should harmonize the actions they may take in response to the reporting of a major incident. ▪ National Competent Authorities should harmonize the supporting measures they may take to help providers solve an incident more quickly or mitigate its impact. We would propose that major incidents reported be anonymised and shared with providers; this would provide them with interesting data on the incident itself and the modus operandi and, in turn, allow them to prevent similar incidents in the future. **Regarding information sharing among private companies and with public authorities:** ▪ Information on incidents should be reported not only to supervisors and regulators. It would add value to the market if this information was also shared between companies on a confidential basis. In particular, sharing information or distributing early warnings on major incidents between financial 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. A similar initiative should be set up at EU level, led by ENISA together with the ECB and EUROPOL. ▪ National data protection rules and confidentiality requirements may act as a potential barrier to sharing threat intelligence where personal data is involved. The different interpretation of privacy guarantees in the various European countries creates difficulties in managing the necessary exchange of cyber threat intelligence among private companies. For example: the IP address of the attacker has to be reported to the national competent authority in Spain but it cannot be shared with other private companies for cybersecurity purposes because it is considered personal data. This is critical to prevent the wide spreading of cyberattacks. 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.Law enforcement agencies (LEAs) could play an important part in improving cross-country collaboration in the exchange of information which is necessary in preventing, detecting, containing, and resolving cyber-attacks and cyber fraud.

		▪ Any initiative on data sharing in the EU should also take into account the international dimension and focus on the creation of a common taxonomy that eases the sharing of information on incidents among regulators, supervisors and companies. ▪ In addition, it would be necessary to: - set up stronger EU cooperation mechanisms between Member States, including at operational level - promote a stronger public-private cooperation in cybersecurity - achieve a stronger cooperation between different authorities and communities (e.g. between CERTs and law enforcement authorities). As stated in answer to question 4.7, the creation of a one-stop-shop mechanism for incident reporting would ease compliance with notification obligations set by GDPR, PSD2, NIS and other regulations affecting financial activity.
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)?	The banking regulatory context itself already highlights the methods for identifying the most efficient penetration tests, namely identifying them through analysis of ICT risks. The possibility of European coordination is highly complex where specific technological and technical aspects exist which make it difficult to have a valid penetration test for everyone. Moreover, too much coordination or standardization of testing can prove risky as the repetition of the same pattern can result in vulnerability. We are supportive of EU level penetration testing if done correctly, i.e. along Global FMA guidelines, to the extent that it would further regional coordination. We are also supportive of a safe and scalable approach to regulatory penetration testing and red teaming across the entire EU wherein single test results satisfy multiple supervisors' requirement (hence limiting the operationally risky execution of penetration tests or red team assessments) Penetration tests by third parties introduce operational and data risks. We support firms conducting their own penetration tests in partnership with the regulatory community, based on the framework GFMA has developed. Standardization of the penetration testing and red teaming operations could potentially lead to lowering of the quality of the process. On the other hand, the establishment of a framework which provides general guidelines for penetration tests and red teaming such

		as OWASP could be an area for consideration. Additionally, it would be beneficial to provide a certification-of-quality for penetration test/red teaming teams which are members of the banking institute's faculty. Finally, the "right to penetration test" (same as the "right to audit") by the banking institutions should be established towards the FinTechs. The rest of players in the industry such as FinTech companies, hardware and software manufacturers as well as SMEs should be subject to similar requirements. Additionally, having some type of non-compulsory but incentivised certification or labelling system similar to quality or energy efficiency certifications around the world could help to increase general cybersecurity levels. Finally, free awareness and training campaigns for those companies that are detected (under some type of prioritization scheme) as the weakest links in the chain would be useful.
Other potential applications of FinTech going forward		
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?	Currently, EBF has not identified other applications of new technologies to financial services, beyond those mentioned above, which can improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing.
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? **(Yes/No/Don't Know- not relevant)**	**NO** Beyond those mentioned above, currently we have not identified other 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

	Please elaborate on your reply to whether there are 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?	

About the EBF:

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

For more information contact:

Noémie Papp
Senior Policy Advisor - Digital & Retail
n.papp@ebf.eu
+32 2 508 37 69