



EBF Response to EBA DP on FinTech

6 November 2017

EBF_029702

EUROPEAN BANKING FEDERATION'S RESPONSE TO THE EBA DISCUSSION PAPER ON FINTECH

The European Banking Federation is submitting a response to the European Banking Authority's consultation with the aim 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.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

 www.ebf.eu

Key points:

◆ **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, in line with the definition¹ proposed by the Financial Stability (FSB) in its report on Fintech published in June 2017² and the one proposed by the Basel Committee for Banking Supervision (BCBS) in its consultation document published in August 2017³. 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. Banks are also FinTech companies.

◆ **Consumers protection, innovation, security and financial stability are key priorities**

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.

¹ “technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services”

² *Financial Stability Board’s Report “Financial Stability Implications from FinTech”, 27 June 2017*

³ *Basel Committee for Banking Supervision’s consultative document on “Sound practices: Implications of fintech developments for banks and bank supervisors”, August 2017*

◆ **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. The principle of “**same services/activities, same risks, same rules and same supervision**” should always be applied in order to ensure consumer protection and market integrity. Regulation should also be 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. 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.

EBF position:

N°	Questions	Answer
AUTHORISATION AND REGISTRATION REGIMES AND SANDBOXING/ INNOVATION HUB APPROACHES		
1	1. Are the issues identified by the EBA and the way forward proposed in section 4.1 relevant and complete? If not, please explain why.	<p>The European Banking Federation (EBF) agrees with the European Banking Authority’s proposed way forward, which we find particularly relevant. We would however like to make the following comments:</p> <p>◆ <u>On consumer protection and the need for a true level playing-field:</u></p> <p>Considering the emphasis that supervisors and regulators place on the need for high levels of consumer protection, the presence of so many unregulated entities (53% non-supervised) suggests that further investigation is required to ensure that entities are treated equally.</p> <p>In this respect, we would like to stress the importance to follow the “same services, same risks, same rules, same supervision” principle. We need to ensure that the regulation and supervisory systems cover the new players in financial services and is applied consistently for the same activity and throughout Europe, regardless of whether the players are financial or not, without hampering Innovation.</p> <p>Indeed, as level playing field is key to ensure not only fair competition but also consumer protection, the same regulatory conditions and supervision should apply to all actors who seek to innovate and compete on FinTech: incumbent banks, FinTech start-ups and Big tech firms. This should ensure consumer protection and market integrity. As the value chain includes different kind of actors and becomes more complex, all firms should go through the same process from product and service design to sales to avoid any regulatory arbitrage in responsibility-sharing. As an example, a compulsory minimal framework of internal controls and compliance according to the complexity and the size of the players could be set up.</p>

◆ **On the sandboxing/ innovation hub approach:**

The EBF is also in support of the activities proposed by the EBA for 2017/2018 especially the inventory and assessment of different Sandbox regimes, to avoid regulatory arbitrage between different Sandbox-regimes in Member States and maintain a level-playing field within the European Union.

Currently we observe that supervisory authorities have a diverging approach on this issue, as the desire to attract innovative companies to their countries drives regulators to make their approach to FinTechs more favourable.

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 or other differences between countries which force suppliers to build all kinds of add-ons to take care of national particularities. 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; Cooperation between financial and non-financial regulators is particularly important in this regard. Most likely we will see FinTech-start-ups establishing themselves in the financial value chain without the need to comply with financial regulation but to comply with other types of regulations (e.g. the GDPR). Without any coherent approach among financial regulators and non-financial regulators (e.g. National Data Protection Authorities), there will be a risk to have legal inconsistencies and regulatory arbitrage.
- 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.

Moreover, we believe that participation in potential sandboxes should not discriminate based on the entity size, but rather let all types of entities participate on equal terms. Therefore, work to further assess the features of sandboxing regimes, innovation hubs and similar regimes is supported. Thus, we welcome the EBA move forward with guidelines in this area and look forward to the final report.

◆ **On Payment Services Directive 2:**

Regarding point 74.c), we believe it is too early to say whether or not to change the guidelines on authorisation of payment institutions under Payment Services Directive 2 (PSD2) to a regulatory Technical Standard (RTS). In case the EBA decides to assess the merits of converting the EBA guidelines on authorisations under PSD 2 into RTS in order to ensure compliance and to identify and certify entities to safeguard high levels of consumer and data protection, it will be advisable to monitor the development in the years to come, before deciding whether or not to change the guidelines to a RTS. This assessment should also take national regulation into consideration.

As an additional point, we would like to stress is the need for the EBA to take also into account in its future analysis the conduct of other entities which could cause concerns for consumer protection, security and the overall stability of the market given their size, brand and deep knowledge of their customers' behaviour (so-called Google Apple Facebook Amazon (GAFA)). If these tech giants decide to enter the EU financial services sector, they can potentially combine the use of their client's data with additional data they can acquire, thanks to new opportunities offered by the incoming EU regulations (such as, for example, by acting as Account Information Service Providers (AISP) or Payment Initiation Service Providers (PISP) under the PSD2 or by taking advantage of the new principle of "data portability", provided by the General Data Protection Regulation (GDPR).

PRUDENTIAL RISKS AND OPPORTUNITIES FOR CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS

PRUDENTIAL RISKS AND OPPORTUNITIES FOR CREDIT INSTITUTIONS

2	<p>Are the issues identified by the EBA and the way forward proposed in subsection 4.2.1 relevant and complete? If not, please explain why.</p>	<p>The EBF supports the EBA's proposed way forward of conducting in-depth analysis of the risks and opportunities for credit institutions, workshops and training for supervisors and possible updates to relevant EBA Guidelines. A comprehensive assessment of the FinTech landscape and the opportunities and risks it entails for credit unions will provide a framework to ensure the best outcomes for the users, companies developing FinTech and banks. We note that the Basel Committee for Banking Supervision (BCBS) is currently also doing work on the risks associated with FinTech. We recommend strong cooperation between the EU policymakers and the BCBS with respect to developing and harmonising policy approaches to address FinTech and ICT risk. At the same time banks have developed and are continuing to improve their governance structures and risk management processes for new technologies. Therefore, the banking sector should be closely consulted with.</p> <p>While we find the issues identified in subsection 4.2.1 both relevant and comprehensive we would like to provide the following recommendations:</p>
---	---	--

◆ **Reviewing the prudential treatment of technical innovation in financial services to ensure incentives and a level playing field**

When reviewing the rules for banks and for banking-like services provided by FinTechs it should be ensured that the same rules apply for the same activities regardless of the entity. FinTech activities are usually subject to more stringent regulation when they are performed within a banking group than if they are provided by other types of institutions. Supervisors should consider where there are banking-like services to apply similar licensing, prudential rules as well as deposit insurance and recovery and resolution requirements. It would be useful to also consider if any potential system-wide issues could arise bearing in mind that new actors often tend to choose the optimum legal structure to avoid the heavy regulatory burden of the financial sector. Small structures may be more exposed than credit institutions to some kind of risks (cyber risks for example). The EBF would support a technological neutrality, proportionality, and market integrity approach

Furthermore, policy makers should explore existing rules to ensure if they indeed set the right incentives for innovation in financial technology and provide a level playing field between sectors and jurisdictions. In that regard, we would like to highlight the capital treatment of investments in software and the treatment of internet access accounts in the Liquidity Coverage Ratio under the Capital Requirements Regulation (CRR).

a) Software investments:

Banks contribute to the digitalisation of the EU economy and software has become a core asset for the banks business models around the world. Banks need to invest in software development to remain competitive and to strengthen their cybersecurity. However, software investments remain penalised in Europe compared to the United-Sates (US), where software is generally risk weighted as an ordinary asset, like premises and equipment. The fact that every euro that an EU bank invests in own software 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 start-up companies are not only a major competitor but also partners for the European banking sector. However, when a bank acquires a FinTech start-up, its main asset- the software, is automatically depreciated given the deductibility that has to be applied to calculate capital levels for banks. If the buyer would be a non-bank, the deductibility would not take effect. As a matter of example, this method is like assigning a zero value to the search engine

of Google if it were bought by a bank. Because of this, banks may be less open to financing these companies.

In EBF's view, it would be disproportionate to put European banks in a competitive disadvantage to their US peers and new players in the market, such as BigTechs. Hence, we suggest that software, being an intangible asset, should not be deducted from CET 1. This exception should be introduced in Article 36(1)(b) Capital Requirement Regulation. Artificial hurdles to EU banks investing in digital should be removed, creating value for the economy as a whole and leading worldwide innovation in the area. Evidence clearly indicates that software has value even in the case of liquidation of a bank.

b) Internet deposits and higher outflows in the Liquidity Coverage Ratio (CRR):

Another example where banks see themselves disadvantaged vis a vis international and non-regulated competitors, is that internet only access banks should be given higher outflow rates in the Liquidity Coverage Ratio calculation as it is considered a high risk channel according to the EBA Guidelines on retail deposits subject to different outflows for purposes of liquidity reporting under Regulation (EU) No 575/2013, on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (Capital Requirements Regulation – CRR).

The use of internet based distribution channels has increased substantially. This makes the assumption that this channel leads to higher outflow rates questionable. The popularity of digital channels is such that almost all banks see this as a key area where they can better serve their clients' needs, by offering them time and location independent services. Many banks have stated they will be focusing on enhancing the web based services in the years to come. This is also underlined by the popularity of mobile banking on smartphones and tablets. Mobile banking is already the primary source of client contact for a number of banks that used to be primarily 'bricks and mortar' banks. Furthermore, customers that have an internet access to their banking account are not only those ones that have opened a deposit online; in fact, also those deposit retailers that initially set up a new contract directly at branches, may additionally require to open an online access for the same banking account. With regard to the possibility to react remotely and instantaneously to market movements, it is true that through internet the risk is higher in terms of time, but however also for customers that have no access to their accounts online, they may close deposits or transfer their cash balances in a short time horizon (hours). The decision to

transfer the available cash is independent from the fact that the client has online access to its account. For these reasons, there is not a great difference if a depositor has also internet access, taking into account that the Liquidity Coverage Ratio is computed on a 30-day horizon. If this risk factor will be maintained, banks will have no incentives to use and promote this type of deposit, with the consequence that they may stop to offer these online accounts. Against this backdrop, the availability of internet as a channel to interact with the customer should in itself not result in higher outflows. Additional drivers for higher outflows should exist.

c) Remuneration:

Another illustrative example can be found in the remuneration rules under the Capital Requirement Directive. This Directive sets a limit to the ratio between the variable and the fixed salary that financial institutions can pay to certain staff members identified as risk takers. As it stands, the rule considers technological skilled professionals in this category however they do not develop risk-taking activities. These, and other rules on internal governance or outsourcing requirements leave banks in a situation of competitive disadvantage in terms of cost, time-to-market and talent attraction and retention.

Regulators could contemplate either exceptions within the regulatory framework or exclusions from the perimeter of prudential consolidation, as allowed by Article 19 of the CRR.

d) EBA Register under Payment Services Directive 2

In terms of other risks, as commented to the EBA recently in its consultation on the draft RTS on the EBA Register under PSD2, we think there are prudential risks to the ecosystem arising where firms may not have an accurate and up-to-date picture of the regulatory status of the firms they are engaging with (including new third-party firms offering FinTech services such as payment initiation or account information services). This risk exists to both the Account Servicing Payment Service Providers (ASPSP) and, ultimately, the end customer and does not provide the necessary consumer protection in line with the spirit of PSD2. Third party provider (TPP) services have been brought into scope of the Directive and this has been driven by the development of the FinTech market and the growth in internet and mobile payments. Our recommendation (as noted in our response to the RTS consultation) is that the EBA should provide a mechanism for ASPSPs to be able to validate TPP regulatory status and permissions electronically and in near real-time.

The EBA has an important part to play in encouraging harmonisation across the EU, for example as with the EBA Register under PSD2. The EBA needs to set an example by ensuring that its own services are available in time with functionality enabled that can support and promote a reliable, 24x7x365, automated and highly interoperable environment. The EBA Register under PSD2 needs to support a highly automated, sophisticated and largely machine-driven communication layer between competent authorities and a range of firms. This is an essential building block for a thriving FinTech sector across the European Union and is a key enabler for the success of PSD2. We feel the EBA should encourage the highest common denominator, as the harmonised standard across the EU, and not the lowest which will ultimately help both ASPSPs and other firms offering FinTech activities alike.

◆ **Customer behaviour**

One of the main drivers beneath all of the issues mentioned in subsection 4.2.1 is the customer-behaviour driver. Whether or not new FinTech start-ups or new business models will prevail or perhaps even become the dominant business design. This change will, to a large extent, be influenced and decided by the customers.

We support that the EBA considers to further work on identifying the prudential risks and opportunities stemming from new technology. It is however important that the EBA in this work also includes customer behaviour in the assessment of how new technologies is creating prudential risks and opportunities.

◆ **Comprehensive and integrated approach to risk management and supervision**

Any new rules and guidance should fit the existing supervisory framework i.e. the Supervisory Review and Evaluation Process (SREP) and be closely integrated in the existing risk pillars, i.e. operational risk and Anti-Money Laundering (AML). Banks consider FinTech and ICT risks to be part of operational risk, but agree it should be assessed in further detail. To a large extent we find that the guidelines for operational risk and ICT risk cover processes and controls that are already in place in the current approach.

The emphasis should therefore be to focus on the coherence between the operational and ICT/FinTech risk management and assessment processes.

◆ **Overlap and inconsistencies of measures**

The variation in regulation across jurisdictions remains a major challenge for technology risk. For instance, diverging cloud computing requirements make it difficult for banks to set a group policy that would more effectively allow them to control and monitor risk. The EBA should consider how it can encourage harmonisation of regulation in this area, including IT Risk. Overlap and inconsistent requirements should be avoided. For example, the ECB has recently completed a thematic review on cyber risk, a risk that currently falls under the wider umbrella of ICT and FinTech risk. Also, at the international level, with various initiatives from Monetary Authority of Singapore (MAS), Swiss and Irish authorities for example, it would be desirable to establish tighter coordination to minimise overlap and inconsistencies. Members would welcome a call for harmonisation of approaches across jurisdictions and would welcome the EBA's leadership in this regard, especially around topics like cybersecurity which is often a cross-jurisdictional problem. Paragraph 84 recognises only the need for cross-border cooperation across member states. A need or approach for cooperation with other trading blocs (Americas, Asia, Africa), is not mentioned and ought to be, as banking and FinTech offer global services, not confined to the EU.

◆ **Principle of Proportionality**

Financial technology offers both opportunities and risks. These vary based on the market in which a company is operating, the technology being deployed, and the purpose for which it is being deployed. The level of variation means that there is no one-size-fits-all means for managing risk. The best approach will be proportional to the risk incurred. There is a concern among members as to the applicability of the principle of proportionality across different jurisdictions and when applied to global institutions. Currently there are several provisions around proportionality which are not consistent and would duplicate work. Further clarifications as to how proportionality was being judged, especially in the case of global banks would be beneficial. Will proportionality be assessed in the context of the market?

As mentioned earlier further consideration should be given to the principle of "same services/same activities, same risks, same rules, same supervision" for all FinTech companies, with respect to both capital requirements and consumer protection.

◆ **Banks should remain free to manage risks using their own taxonomies.**

While the Risk Taxonomy is designed to unify the Europe-wide review of ICT and FinTech risks, we would wish to see that banks retain latitude to manage risks using their own taxonomies. Firms should be free to use frameworks that they consider appropriate for managing ICT and FinTech risk i.e. to develop a formula or methodology for risk tolerance/thresholds owing to its own measurement of operational and ICT/FinTech risk. These are important points as mandating any taxonomy in the management of risks within firms might remove the opportunity for the management of risk in a way that matches the enterprise-wide approach. Such a move could present a further danger that categories are seen as complete thereby constraining a firm's thinking around its risks. Also, the notion or taxonomy should be clarified, in order to correctly allocate the incidents under the proper ICT risk categories.

◆ **Other remarks (to be considered and if necessary to be elaborated on)**

- **Data protection:** We are surprised that the GDPR is not mentioned in the EBA DP as its impact could be important in particular regarding the responsibility and liability requirements that an effective sharing of data demands.
- **Strong customer authentication:** In the protracted debate over the finalization of the Regulatory Technical Standards on Strong Customer Authentication (PSD 2) it appears that the Commission's ambition to be innovative may at times relegate concerns about consumer protection to a secondary consideration.
- **On Cybersecurity:**
 - Cybersecurity threats remain one of the most important challenges for banks and the EBF supports the EBA proposed way forward. The EU has an important role to play, notably when it comes to streamlining harmonised format and procedures for cyber incident reporting, establishing a legal framework for data (intelligence) sharing and encouraging collaboration between the industry and regulators and among regulators.
 - The following points should however be clarified:
 - It is assumed in the discussion paper (paragraph 78) that the introduction of FinTech translates to increased cybersecurity and fraud, whereas the opposite could easily be

		<p>argued, i.e. that organizations failing to adopt new technologies become easier targets for criminals.</p> <ul style="list-style-type: none"> - Also in paragraph 80 the paper inappropriately links FinTech development with increased cybersecurity risk. The link should be more on inappropriate deployment and insufficient attention to security measures or more related to paragraph 83 on the valid ICT complexity argument ▪ On Cloud: the EBF supports the EBA’s action on cloud computing (please see EBF response to the consultation on the EBA draft recommendations on outsourcing to cloud service providers). While we appreciate the EBA’s efforts to adapt outsourcing recommendations to the specificities of cloud computing technology, we however believe that the instrument used (EBA recommendations, that by nature are not directly applicable nor mandatory in a first instance) could introduce an element of divergence and lack of harmonization across Member States. To avoid this, technical standards or any other directly applicable instrument would have been a better option. <p>It should also be perfectly clear that neither these EBA recommendations on cloud outsourcing, nor the whole Single Supervisory Mechanism (SSM), applies to cloud outsourcing by financial institutions that are not under the SSM, even though the parent company is under the SSM. Instead, outsourcing by financial entities that are not under the SSM must be ruled by local outsourcing and local data protection rules. With reference to paragraph 82 of this discussion paper, we believe it would be helpful to establish a common cloud risk framework to be applied across the EU to assess and mitigate risks of data and services transfer to the cloud, to be tailored to the different service and delivery models. Such a framework could help companies evaluating risks based on the same criteria adopted by cloud service providers (CSPs).</p>
3	<p>What opportunities and threats arising from FinTech do you foresee for credit institutions?</p>	<p>Technology in and of itself is neither positive nor negative. Social benefit will only accrue from how technology is used by both regulated and non-regulated market players. In our view, the EBA has well evaluated the opportunities for all the stakeholders resulting from technological innovation. As underlined in the discussion paper, in reason of the competitive pressure stemming from other operators entering their traditional markets, the business risk appears to remain one of the most important risks to manage for credit Institutions.</p>

Winning the customers will be crucial in deciding which FinTech companies (large, small, old or new) will prevail. The Basel Committee for Banking Supervision (BCBS) has in its consultative document '*Sound practices: Implications of FinTech developments for banks and bank supervisors*' (page 16)' presented 5 scenarios, that lays out possible outcomes of the coming battles among FinTech companies to win the customers. In our opinion the 5 scenarios constitutes a good description of both the opportunities and risks that are foreseeable. We do see that some of the 5 scenarios will possibly play out simultaneously, because of differences between banks and their level of digitalisation and difference in their innovations capabilities.

Differences in the regulatory treatment of FinTech Firms and particularly between regulated and non-regulated entities could create distortions of competition that could unfairly exacerbate the competitive pressure.

As expressed previously, in any foreseen action or regulation, the principle 'same service, same risk, same rules, same supervision' should apply. The issue should also be assessed globally. European banks should not be weakened on the global scene. As underlined in the study of the World Economic Forum, globally there are differences in the regulatory priorities. It is given the example of the strong regulatory impetus for open data and consumer protection in Europe putting incumbents under growing pressure.

◆ **As reminded in the discussion paper, the growing importance of cloud services as a driver of innovation has led the EBA to develop draft recommendations on the use of cloud services by credit institutions and investment firms.**

The recommendations of the EBA are essential but should be replaced in the context of the cloud industry.

While technology in banking has adapted to business requirements within the legal and regulatory constraints applicable at local, national and regional level, banks have nevertheless been seen to be slower in migrating services to the cloud when compared to other industries. 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).

For the banking sector, cloud adoption must be considered within the context of maintaining regulatory compliance. Outsourcing institutions/banks therefore typically approach compliance assurance with Cloud Service Providers (CSPs) through specific contract clauses, Service Level Agreements (SLAs), certifications and audits. The lack of specific and detailed information drives banks and suppliers into a difficult situation: banks are generally forced to evaluate, on their risk assessment criteria basis, whether the provider solutions are adequate in terms of compliance (e.g. in terms of IT security). Banks have thus to make the choice of either rejecting the supplier or accepting the risks that cannot be fully mitigated.

This entire situation creates important barriers to the full adoption of cloud solutions by the banking sector as a whole.

Without limiting the CSPs' contractual freedom to negotiate specific conditions/clauses in line with their business model, the development, with the industry, of high-level principles covering the specific needs of the banking sector with the aim to also accommodate GDPR requirements, should be encouraged to guarantee legal certainty and facilitate the adoption of the cloud by financial institutions. For example, the contract between a bank and a CSP should include availability, reliability and confidentiality SLAs but leave open for the bank to decide which SLA to include.

Another key factor slowing down cloud adoption in Europe is the lack of harmonisation in 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.

In addition, the adoption of cloud is also slowed down by 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. Not least to maintain trust and confidence of the financial system. If privacy and security measures are breached, the consequences will negatively impact the reputation of banks. What is more, they would most certainly be devastating for banks' customers.

Besides the need for harmonisation among EU financial supervisors outsourcing regulation, there is a need to bring agility to the cloud adoption process, reducing time to market to increase competitiveness.

In our view, a description on how systemic risks (domestic, international) should be handled, is missing. Third-parties' certifications would help financial institutions to rely on a standard approach across Europe. The adoption of base standard certifications to guarantee compliance or the definition of a cloud outsourcing banking standard against which a certification could be requested, would help financial institutions and CSPs across Europe to reduce the compliance burden and increase security. A more detailed reference to a base standard certification would help. In our view CSPs should have the same execution framework with all their clients (including banking institutions) and should be certified by a Regulator.

An additional threat will come from platforms (distribution, segment, data aggregation) including those characterized as GAFAs. This threat has not been identified by the EBA, and should be added.

◆ **Overview of Opportunities and Risk for banks**

As mentioned previously, the Basel Committee for Banking Supervision (BCBS) has in its consultative document '*Sound practices: Implications of FinTech developments for banks and bank supervisors*' issued a highly valuable assessment of the risks and opportunities from FinTech in five future potential scenarios. See below the issues that were identified with some complementary issues added by our Members.

Opportunities

- Improved and more efficient banking processes for example:
 - closer connection and faster response to customer needs (digitalisation)
 - lower operating costs (efficient and innovative solutions);
- Innovative use of data for marketing and risk management purposes i.e. increased transparency on business transactions and processes;
- Potential positive impact on financial stability due to increased competition;
- Innovative technology can facilitate compliance with regulation e.g. faster replacement of security-prone legacy systems (cyber security improvement).

Risks

- Exposure to non-regulated entities;
- Strategic and profitability risks;
- Increased interconnectedness between financial parties;
- new operational risk scenarios – systemic and idiosyncratic;
- Third-party/vendor management risk;
- Compliance risk including failure to protect consumers and data protection regulation;
- Money laundering – terrorism financing risk;
- Liquidity risk and volatility of bank funding sources;
- Insufficient control assurance: through insufficient right-to-audit, or over-reliance on insufficient audit information;
- Loss of control of information assets (especially customer data) which could cause an information asymmetry;
- Obsolete FinTech regulations not keeping pace with Fintech innovation;
- Insufficient response to technology issues: More complex event, incident/ disaster and problem management chains;
- Late adoption leading to opportunity loss;
- Supervision and regulatory asymmetry.

RISKS AND OPPORTUNITIES FOR PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS

4	<p>Are the issues identified by the EBA and the way forward proposed in subsection 4.2.2 relevant and complete? If not, please explain why</p>	<p>The European Banking Federation (EBF) agrees with the European Banking Authority (EBA)'s proposed way forward and the range of EBA work planned.</p> <p>In addition, the EBF supports the EBA ongoing work on identifying the prudential risks and opportunities. It is however important in our opinion to also include customers and their behavior at the heart of the assessment of how new technologies are creating prudential risks and opportunities.</p> <p>Moreover, the products and services are all expected to change at a rapid pace, therefore it is sensible that security solutions and frameworks remain agile. One way of achieving this is by ensuring that various regulation (level 1, level 2 text, etc.) are kept technology neutral, but also to avoid large time gaps between the finalization of level 1 and level 2 texts. We notably support that the EBA will continue to develop and implement security-related products under the Payment Services Directive 2 (PSD2).</p> <p>The EBF believes Distributed Ledger Technology (DLT) could be a technology which assists the processes between where information is exchanged, particularly where no central dedicated infrastructures exist. DLT based technologies could also help banks to streamline their processes and achieve substantial back-office cost savings. There are opportunities in financial services infrastructure for close collaboration to create economies of scale and better processes through automation. There are a number of projects currently underway in which the various industry players cooperate on industry-wide solutions, these include consortia as well as looser alliances.</p> <p>The EBF therefore supports the EBA approach to assess the risks and potential benefits arising from DLT in the payment markets.</p> <p>The EBF also supports EBA's plan to have workshops and trainings for supervisors on DLT. At this stage, and considering the maturity of the technology, it is fundamental to fully and properly understand the functioning of DLT and all its possible applications in the financial sector.</p> <p>Therefore, we remain available to arrange targeted workshops with regulators in order to present the work that banks are currently undertaking on DLT in the payment market space.</p>
---	--	--

5	<p>What opportunities and threats arising from FinTech do you foresee for payment institutions and electronic money institutions?</p>	<p>◆ <u>On the prudential risks and opportunities for payment institutions and electronic money institutions:</u></p> <p>Payment institutions and electronic money institutions are subject to regulatory frameworks that affect the provision of many of their services. However, as the EBA notes in its mapping study, many other players participating in payment markets may not be regulated. This difference in regulatory treatment may result in a distortion of competition for this activity as some players may benefit from the existence of regulatory loopholes.</p> <p>A clear example of this could be the EBA’s opinion in 2014, that called on national supervisory authorities to prevent credit institutions, payment institutions and e-money institutions from buying, holding or selling virtual currencies; thus, creating asymmetries. Regulating the activity of virtual currencies is necessary to ensure a level playing-field and eradicate asymmetries in financial markets.</p> <p>As stated above, avoiding fragmentation within the EU is of key importance. This is also the case in relation to the Payment Services Directive 2 (PSD2). The EBF supports the objectives of the Directive but its technical implementation runs the risk of fragmentation within the EU, to the detriment of security and efficiency. This is particularly the case for the central register, the reporting of fraud and major incidents that leave excessive room for discretion to national competent authorities. We therefore believe that additional work by European institutions (EBA, together with the European Commission and the European Central Bank) is urgently needed to support the payment industry in the implementation of PSD2.</p> <p>In addition, in its August 2017 report - entitled “Beyond FinTech: a pragmatic assessment of disruptive potential in financial services”- the World Economic Forum (WEF) recognized that payments businesses are experiencing intense pressure and a challenging regulatory environment. It also points out that the regulatory ecosystems are evolving very differently across jurisdictions and that this could lead to regional distinctions between payments ecosystems.</p> <p>As stated by the WEF, the application of the PSD2 will bring a great shift in the European payment landscape that are very unlikely to be followed or influence other regions’ regulations. For instance, US actors are currently growing and could take advantage of the current curtailing of financial institutions’ control over access to infrastructure, lowering market power and shifting profits away from firms that oversee infrastructure.</p>
---	---	---

Indeed, US companies' global position, their large customer base and use of a vast amount of information about their customers enable them to provide more tailored services to consumers thus giving them a competitive advantage over their competitors.(

The European regulators should pay attention and keep in mind these facts in order to better defend European actors on the global stage.

◆ **On Distributed Ledger technologies:**

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).

A concrete example on the payment side is the possible application of the technology on Real Time Payments. Today the financial industry, outside of the Single Euro Payments Area (SEPA) area, 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 DLT-based payment protocols available on the market and experimenting with a proof of concept platforms. These solutions take advantage of the capabilities of DLT to execute payment obligations netting and enable real-time clearing without the involvement of correspondent banks on each transaction.

Furthermore, the EBF believes DLT might be complementary to Application Programming Interfaces (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.

		<p>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.</p> <p>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.</p> <p>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.</p> <p>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/ Service-Oriented Architecture (SOA)/Public Key Infrastructure (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.</p>
--	--	--

THE IMPACT OF FINTECH ON THE BUSINESS MODELS OF CREDIT INSTITUTIONS, PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS

IMPACT OF FINTECH ON INCUMBENT CREDIT INSTITUTIONS’ BUSINESS MODELS

6	<p>Are the issues identified by the EBA and the way forward proposed in subsection 4.3.1 relevant and complete? If not, please explain why.</p>	<p>The European Banking Federation welcomes the proposed way put forward by the European Banking Authority in its discussion paper to better understand the impact on credit’s institutions’ business model.</p>
---	---	--

We would first like to note that it is important not to oppose “FinTech” and credit institutions, payment institutions and electronic money institutions. Credit, payment institutions and electronic money institutions have been the main channel of technological innovation for decades.

Many of the developments, which have been rolled out over the years to banking services consumers, would today be called ‘FinTech’. The examples range from chip cards, contactless payment cards, the availability to make mobile payments, including all the features developed for online and mobile banking, to less visible and obvious developments, like the development of cloud computing, all the while benefiting consumers.

From a geostrategic point of view any framework developed in Europe should facilitates innovation counting on the strength of all FinTech firms (banks, non-banking FinTech/ FinTech start-ups). In this context, it is important to ensure that the regulation, which represents another challenge in itself (with significant investments at stake), will not hinder incumbents’ ability to innovate and transform themselves or disadvantage them (distortion of competition). We thus welcome the EBA’s consideration to further analyze the relationship between incumbent credit institutions and new players.

Importantly, we would like to point out a couple of issues in relation to the paragraph 94:

- The EBA is in our views wrong in stating that “credit institutions may have to move from a ‘product/channel centric approach’ towards a ‘customer centric approach’”. This is not something that *may* happen but that has already happened. First and foremost the evolution of customer behavior and expectations drives and have always been driving the transformation of banks.
- The EBA also states that “*credit institutions may be forced to adapt their business models in response to the increasing competition from FinTech*”. We believe this is a misconception. As stated above, FinTech and banks should not be opposed, the broad FinTech definition that rests on the innovative application of technologies encompasses also banks. As a result, business models need to be adapted due to the application of FinTech by financial institutions’ competitors, regardless of the entity.

		<p>As regards paragraph 96 of the EBA Discussion Paper on the expansion of FinTech companies into low profitability environments, we believe it is important to stress that it is key for both established companies and start-ups.</p> <p>This move will increase the industry as a whole by supplying financial credit products to companies or individuals that have not been catered to in the past. We believe that this move will, to a substantial degree, be done through partnerships between established financial companies and new entrants and that it will reduce time-to-market and costs as well as improve the quality of the products and services.</p> <p>Moreover, it is important to evaluate the attitude supervisors have to a progressive regulatory approach to innovation, no matter the size of the innovator. That is why we believe that communication with innovators, no matter their size, is key to understand the impact of the innovative products and services on consumer protection and whether the product or service actually needs to be regulated</p> <p>◆ <u>On distributed ledger technology:</u></p> <p>Distributed Ledgers 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/Know Your Customer (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.</p> <p>The EBF stands ready to support the EBA and facilitate its work in conducting interviews with representatives of credit institutions.</p>
7	<p>What are your views on the impact that the use of technology-enabled financial innovation and/or the growth in the number of FinTech providers and the volume of their business may have on the</p>	<p>When approaching this phenomenon, it is important to understand what types of FinTech exist, as this term covers a wide range of companies and solutions. In the new FinTech ecosystem, composed of banks, new entrants, BigTech companies and regulators, the lines between competition and collaboration are blurring. Whilst a number of institutions are actively pursuing an innovation agenda, some aspects of existing requirements restrain their ability to innovate. As expressed earlier, we observe that emerging technological players who now provides financial services do not have to comply with prudential regulations imposed on the banking sector or/and</p>

<p>business model of incumbent credit institutions?</p>	<p>current prudential rules are not adapted to the digital reality /do not take into account the digital transformation of the banking sector. For example, 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.</p> <ul style="list-style-type: none"> ▪ 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 (please see more in our response to question 2). ▪ 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.
---	---

		<p>Regarding DLT, currently it is extremely difficult to assess thoroughly the impact of the 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.</p> <p>In parallel, a solid business case should be built to understand what are the conditions upon which the use of such technology would create value for each use case.</p>
--	--	--

IMPACT OF FINTECH ON INCUMBENT PAYMENT INSTITUTIONS AND ELECTRONIC MONEY INSTITUTIONS BUSINESS MODELS

8	<p>Are the issues identified by the EBA and the way forward proposed in subsection 4.3.2 relevant and complete? If not, please explain why.</p>	<p>The European Banking Federation welcomes and supports the EBA’s proposed way forward. Indeed, it makes sense that the work conducted by the EBA on the business models of credit institutions be expanded to include in its scope payment institutions and electronic money institutions.</p> <p>As mentioned earlier, in our views, the best way to foster innovation is to apply the principle “same services, same risks, same rules, same supervision” regardless of the entity.</p> <p>As expressed in question 6, it is important not to oppose “FinTech” and credit institutions, payment institutions and electronic money institutions. Credit, payment institutions and electronic money institutions have been the main channel of technological innovation for decades. Many of the developments, which have been rolled out over the years to banking services consumers, would today be called ‘FinTech’.</p> <p>The examples range from chip cards, contactless payment cards, the availability to make mobile payments, including all the features developed for online and mobile banking to less visible and obvious developments, like the development of cloud computing, all the while benefiting consumers.</p>
---	---	--

It is important to recall that 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);

		<p>h) Corporate and Investment Banking, SME banking solutions, IT core banking solutions, and solutions focused on enhancement of data quality and the data architecture.</p> <p>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.</p> <p>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.</p> <p>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</p> <p>However, these new technologies and services are not always developed exclusively by incumbents. There are thus great opportunities in creating and nurturing an innovative ecosystem where actors, both start-ups and incumbents, collaborate and innovate together to the benefit of consumers and the economy at large.</p> <p>In addition, attention should be given to "indirect support" (skills): developing and acquiring the right digital talent and skills within the EBA is the best way forward for European policy making to keep pace. Business models will continue to evolve rapidly and regulators will need to respond by adapting supervision models. One challenge will be for regulators and supervisors to have access to the correct skills. Therefore, effort should be spent on developing skills and talent among existing staff, offer training, etc.</p>
9	<p>What are your views on the impact that the use of technology-enabled financial innovation and/or the growth in the number of FinTech providers and the volume of their business may have on the</p>	<p>The arrival of FinTech start-ups has spurred innovation, accelerated the transformation of banks and opened new doors for collaboration benefitting all parties. As mentioned in question 8, the complementary strength of both banks and start-ups in FinTech mean that they will often do better by cooperating rather than competing.</p>

	<p>business models of incumbent payment or electronic money institutions?</p>	<p>In the payment space, FinTech could bring some new solutions:</p> <ul style="list-style-type: none"> ▪ Distributed ledgers Technology: DLT can provide for the development of more efficient trading platforms and payments systems. DLT is the innovation where collaboration with other market players will most be needed as no DLT system will be possible without global and far-reaching collaboration ▪ Real time payments: A number of banks have been reviewing new DLT-based payment protocols available on the market and experimenting with a proof of concept platforms. These solutions take advantage of the capabilities of DLT to execute payment obligations netting and enable real-time clearing without the involvement of correspondent banks on each transaction. ▪ 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. <p>It should also be noted that retailers, both large and small, are very likely to have a decisive influence on how the future business models of payment and electronic money institutions will evolve.</p> <p>Whilst a number of institutions are actively pursuing an innovation agenda, some aspects of existing requirements restrain their ability to innovate. 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. For instance, the current regulatory capital framework for credit institutions does not recognize the value of software for capital purposes. (Please see our comments to question 7).</p> <p>From the point of view of Security, guidance from supervisors on which standards to follow, such as NIST, ISO 2700X or COBIT would ease compliance. In addition, authorities can be helpful by delivering the Regulatory Technical Standards in advance to allow sufficient time for the industry to adapt.</p>
--	---	---

CONSUMER PROTECTION AND RETAIL CONDUCT OF BUSINESS ISSUES

UNCLEAR CONSUMER RIGHTS DUE TO UNCLEAR REGULATORY STATUS

10	<p>Are the issues identified by the EBA and the way forward proposed in subsection 4.4.1 relevant and complete? If not, please explain why</p>	<p>The European Banking Federation agrees with the way forward proposed by the European Banking Authority. The establishment of a clear regulatory perimeter will be a positive step towards solving the problem of customers not being able to determine who they are dealing with and how their rights would be protected.</p> <p>Current asymmetries hinder innovation and create risk situations (e.g. quality of information, cybersecurity etc.) for consumers who do not have a homogeneous level of protection, but also for all the financial institutions.</p> <ul style="list-style-type: none"> ▪ This is the case, for instance, of marketplaces in which consumers can directly sign up to products from different providers. In this context, the lack of a regulatory framework generates uncertainty about the allocation of liabilities, and whether the responsibility lies with the provider or with the platform. As platforms are not regulated, this would ultimately lead to an overburden of the liability on the providers, which are regulated figures. ▪ Financial institutions can also be directly affected by fraud problems linked to cyber security issues encountered by certain actors, or more indirectly by the weakening of the consumer confidence in financial services. ▪ Another example would be the comparison websites that show financial information in a manner that may not always be fair or complete. <p>When conducting comparison, information, recommendations, advisory services or distribution services online a clear distribution of responsibilities is needed as well as oversight by financial authorities.</p> <p>It is also important to stress that innovations are indeed valued differently depending on the different countries' authorities.</p>
----	--	--

		<p>As an example, IDnow's videoconferencing solution used by Number 26 in Germany has been approved by the BAFIN as a possible means of remote identification when in other countries such solution is not accepted by the national authorities, creating an unlevel playing field among the various actors but also among countries.</p> <p>Given that in the digital space the boundaries among sectors are unclear and new business models appear constantly, a prerequisite is to ensure that consumers are protected and that the financial stability is ensured, irrespective of who the provider is (including for example FinTech companies that lawfully are established without any licensing). A level playing field regarding the regulation of potential competitors/sectors and between Members States should be guaranteed, in particular when issues such as KYC, digital signature, MiFID are addressed. It is of paramount importance to adopt an activity based approach regardless of the channel or the institution offering it. The principle of "same services/activities, same risks, same rules and same supervision" should apply, otherwise, users of the same financial service could end up being subject to different levels of protection depending on whether the service is provided by an incumbent or a new entrant and depending of the country.</p> <p>Regarding paragraph 74.c), we believe it is too early to say whether or not to change the guidelines on authorisation of payment institutions under PSD2 to an RTS. In case the EBA decides to assess the merits of converting the EBA guidelines on authorisations under PSD 2 into RTS in order to ensure compliance and to identify and certify entities to safeguard high levels of consumer and data protection, it will be advisable to monitor the development in the years to come, before deciding whether or not to change the guidelines to a RTS. This assessment should also take national regulation into consideration.</p>
--	--	---

UNCLEAR CONSUMER RIGHTS IN THE CASE OF CROSS-BORDER PROVISION

11	<p>Are the issues identified by the EBA and the way forward proposed in subsection 4.4.2 relevant and complete? If not, please explain why.</p>	<p>As stated earlier, we believe a level playing field should be ensured for companies engaged in similar activities having similar risks, irrespective of the European country. On any foresee initiatives, the principle "same service, same risk, same rules, same supervision" should apply.</p> <p>The EBF therefore agrees with the way forward proposed by the EBA, in particular:</p>
----	---	---

		<ul style="list-style-type: none"> ▪ Concerning equivalent regulation to be extended to non-regulated firms when providing the same services. For instance, not all European countries have developed legislation for alternative finance, creating a set of diverging regulatory frameworks within the EU. In these cases, new FinTech players trying to operate cross-border face a practical impossibility due to the lack of passporting facilities. ▪ In setting up a harmonized framework for cooperation, setting a clear distribution of competences between home/host supervisors and the EBA playing the role of being a forum for facilitating information sharing. <p>It should however be underlined that, according to many studies, there is a very low demand for cross-border operations, and there are limited examples of products and services being offered in more than one jurisdiction. EBA needs, for instance, to keep in mind that the digital dimension creates challenges for supervisors as both large and small innovative entities might not aim to set up branches or apply for licences in all member states where the services are provided. We observe that consumer protection laws which is a very important component to fulfil when selling products or services cross-borders, are far to be harmonized within the EU Member States.</p>
12	<p>As a FinTech firm, have you experienced any regulatory obstacles from a consumer protection perspective that might prevent you from providing or enabling the provision of financial services cross-border?</p>	<p>As stated above, banks believe that different consumer protection regimes act as a barrier to the provision of cross-border retail banking products and services, both for consumers and banks. Companies need to assess the legal regime to undertake the provision of services on a cross-border basis and in some cases, it cannot be adapted to the legal regime of the country of origin of each potential customer.</p> <p>For example: the development of foreign settlements in French establishments, which are often subject to stricter constraints than their counterparts in the extent to which, in certain aspects, the rules of the two countries, of the establishment and of the parent company) have to be considered.</p> <p>Regulatory fragmentation across Europe regarding digital identity remains a big obstacle for a harmonized European digital identity frameworks, despite the eIDAS Regulation. There is also a lack of an interoperable digital identity system, which creates a problem of fraud and identification. It is key to ensure that identification means are effective and can be used across national boundaries (e.g. in case of videoconference, it is only accepted in a limited number of countries).</p>

		<p>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, in order to guarantee the acceptance of the means for identifying customers in all Member States.</p>
13	<p>Do you consider that further action is required on the part of the EBA to ensure that EU financial services legislation within the EBA's scope of action is implemented consistently across the EU?</p>	<p>For a genuine cross-border retail financial market to operate in Europe, it is key that a harmonized consumer protection framework is developed, also by reforming current national regulations.</p> <p>In our view, no new regulation is required at the moment. It is preferable to make use of existing extensive regulation protecting consumers and give them time to produce their effects and to assess if they apply to all players. Secondly, the impact of new technologies, in terms of benefits and potential risks, has to be studied before deciding on new regulations which may stifle innovation. In line with the principles of better regulation and proportionality, it would be important to evaluate the impact of these measures before introducing new ones.</p> <p>Practical steps that could be taken in this direction, for instance:</p> <ul style="list-style-type: none"> ▪ as mentioned in the previous question, it is key to ensure that identification means are effective and they can be used across national boundaries (i.e. in case of videoconference, it is only accepted in a limited number of countries); ▪ some texts cover only credit institutions. Some specialized or alternative actors, who have pushed for the creation of new accreditation categories in certain countries and for crowdfunding, are not always subjected to the same requirements and supervised in the same way, which creates a distortion and does not guarantee good consumer protection; ▪ With regards to security, financial actors are subject to a specific supervisory regime as a result of their activities, which is more supervised than other sectors. We believe it is necessary to extend the scope of cybersecurity regulation and supervision to all players who offer financial services and manage financial data. The security constraints imposed by regulators must be the same for all actors who handle or collect personal and bank data from end-to-end with the highest level of security (no weak link).; ▪ At European level, the European Commission wants to promote competition and innovation among financial players by "opening up" certain systems. It is necessary that these initiatives not be detrimental to the soundness (and even the "usability") of the systems in place.

		<ul style="list-style-type: none"> ▪ The personal and banking information of our customers must be protected against the leakage of information, in the internal systems but also and especially in the "new actors" who consume this information and when they circulate between actors. This dissemination of information can facilitate identity theft or the development of models based on the monetization of customer financial data; ▪ The responsibility of each of the actors must be clearly defined in the event of an incident. <p>The EBA could also play a role by facilitating consistency between level 1 and level 2, by enabling knowledge and experience sharing among national competent authorities and providing an overview of the transposition of number of EU legislations from a supervisory perspective. This is particularly important, when there is an interim period between the application dates of level 1 and level 2 legislation.</p>
--	--	---

UNSUITABLE OR NON-EXISTENT COMPLAINTS HANDLING PROCEDURES

14	<p>Are the issues identified by the EBA and the way forward proposed in subsection 4.4.3 relevant and complete? If not, please explain why</p>	<p>We agree that the findings of the EBA concerning non-regulated FinTech firms, which may have unsuitability or non-existing complaints, handling procedures should receive attention.</p> <p>Currently regulations tend to assign to incumbent banks the role of "claim concentrator" without fair compensation (notably in PSD2).</p> <p>As far as regulated FinTech firms (banks) are concerned the consumer protection is fulfilled:</p> <ul style="list-style-type: none"> ▪ Thanks to the Alternative Dispute Regulation, low-priced mediation and reconciliation mechanisms will be expanded further. In addition, directives on unfair terms and unfair business-to-consumer commercial practices provide the consumer with sufficient protection from any abusive sale of financial products; ▪ To help consumers to find an adequate redress mechanism in cross-border situations the Financial Dispute Resolution Network (FIN-NET) was founded in 2001. In its green paper, the European Commission is in the view that FIN-NET could be upgraded and that measures should be taken to increase consumer awareness of FIN-NET. As banking industry, we are totally in favour of measures for expanding the use of FIN-NET.
----	--	---

		<p>We also agree that 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.</p> <p>Companies that are not regulated may have less complaint facilities. Therefore, in order to promote customer protection further, the EBA might consider investigating whether non-regulated companies that participate in the provision of financial services or products shall establish similar complaint facilities as regulated entities.</p> <p>Moreover, introduction of one-stop-shop mechanisms could streamline the process of filing complaints for consumers, especially in cases where the financial service is provided through an interaction of various firms with different regulatory status.</p> <p>Another issue that is of relevance here, is how consumer protection regulations interact with financial services that are not offered by providers located in Europe, or that, due to their immaturity, have an uncertain legal nature or a lack a clear legal framework that deals with territoriality or liability issues. This is the case for instance with bitcoin and other digital cryptocurrencies.</p>
--	--	---

INADEQUATE/INSUFFICIENT DISCLOSURE TO CONSUMERS IN A DIGITAL ENVIRONMENT

15	<p>Are the issues identified by the EBA and the way forward proposed in subsection 4.4.4 relevant and complete? If not, please explain why.</p>	<p>The issues identified by the European Banking Authority and the proposed way forward are relevant and complete. Particularly, we appreciate the EBA’s intention to assess whether EU legislation in place generates restrictions to digitalisation of financial services.</p> <p>We believe it is of the utmost importance to replace the use of paper or non-digital-native (e.g. pdf) documents in any form of communication, as the above prevails even in pieces of legislation that have been produced in recent years. Instead, financial institutions should be given the opportunity to communicate with their clients in whatever format is best suited to the client’s needs and to the channel deployed.</p>
----	---	--

		<p>In particular, we support conducting additional work on disclosure requirements. There is a risk of different approaches to disclosure which could act against the customers' ability to compare propositions and any 'hidden' costs associated with the services on offer. We believe a consistent approach to disclosure will promote customers' ability compare information and to make well informed, relevant choices.</p> <p>On paragraph 120, please see some detailed comments below:</p> <ul style="list-style-type: none"> ▪ Paragraph d & f: we believe that there should not be any differences in the regulation of products and services based on the channel that they are being provided through. Any regulation or initiative should be technology neutral; ▪ Paragraph g: new investment products or crowdfunding products may require that certain information is provided to the customer. We recommend that, in these cases, the EBA revert to legislation like MiFID or other relevant texts to better ensure alignment.
16	<p>Are there any specific disclosure or transparency of information requirements in your national legislation that you consider to be an obstacle to digitalisation and/or that you believe may prevent FinTech firms from entering the market?</p>	<p>In general, there are many consumer protection legislations requiring that great amounts of information should be provided to the consumer ex-ante. Here other national requirements, such as the requirement that certain contracts need to be physically signed in a bank branch, also make it more difficult to digitalise certain products and services.</p> <p>Several important pieces of EU legislation also still take a "paper first" approach:</p> <p>◆ <u>Undertakings for the Collective Investment of Transferable Securities (UCITS):</u></p> <p>Article 38 of the Commission Regulation (EU) No 583/2010 of 1 July 2010 implementing Directive 2009/65/EC of the European Parliament and of the Council as regards key investor information and conditions to be met when providing key investor information or the prospectus in a durable medium other than paper or by means of a website states the following conditions should apply:</p> <ol style="list-style-type: none"> 1. <i>Where, for the purposes of Directive 2009/65/EC, the key investor information document or prospectus is to be provided to investors using a durable medium other than paper the following conditions shall be met:</i> <ol style="list-style-type: none"> (a) <i>the provision of the key investor information document or the prospectus using such a durable medium is appropriate to the context in which the business between the management company and the investor is, or is to be, carried on; and</i>

(b) *the person to whom the key investor information document or the prospectus is to be provided, when offered the choice between information on paper or in that other durable medium, specifically chooses that other medium.*

2. *Where the key investor information document or the prospectus is to be provided by means of a website and that information is not addressed personally to the investor, the following conditions shall also be satisfied:*

(a) *the provision of that information in that medium is appropriate to the context in which the business between the management company and the investor is, or is to be, carried on;*

(b) *the investor must specifically consent to the provision of that information in that form;*

(c) *the investor must be notified electronically of the address of the website, and the place on the website where the information may be accessed;*

(d) *the information must be up to date;*

(e) *the information must be accessible continuously by means of that website for such period of time as the client may reasonably need to inspect it.*

3. *For the purposes of this Article, the provision of information by means of electronic communications shall be treated as appropriate to the context in which the business between the management company and the investor is, or is to be, carried on if there is evidence that the investor has regular access to the Internet. The provision by the investor of an e-mail address for the purposes of the carrying on of that business shall be treated as such evidence.*

◆ **Key information documents for packaged retail and insurance-based investment products (PRIIPS) Regulation:**

Article 14 of the Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs) states that :

		<ol style="list-style-type: none"> 1. <i>The person advising on, or selling, a PRIIP shall provide the key information document to retail investors free of charge.</i> 2. <i>The person advising on, or selling, a PRIIP shall provide the key information document to the retail investor in one of the following media:</i> <ol style="list-style-type: none"> (a) <i>on paper, which should be the default option where the PRIIP is offered on a face-to-face basis, unless the retail investor requests otherwise;</i> (b) <i>using a durable medium other than paper, where the conditions laid down in paragraph 4 are met; or</i> (c) <i>by means of a website where the conditions laid down in paragraph 5 are met.</i> 3. <i>Where the key information document is provided using a durable medium other than paper or by means of a website, a paper copy shall be provided to retail investors upon request and free of charge. Retail investors shall be informed about their right to request a paper copy free of charge.</i> <ol style="list-style-type: none"> (a) <i>The key information document may be provided using a durable medium other than paper if the following conditions are met:</i> (b) <i>the use of the durable medium is appropriate in the context of the business conducted between the person advising on, or selling, a PRIIP and the retail investor; and</i> 4. <i>the retail investor has been given the choice between information on paper and in the durable medium, and has chosen that other medium in a way that can be evidenced.</i> 5. <i>The key information document may be provided by the means of a website that does not meet the definition of a durable medium if all of the following conditions are met:</i> <ol style="list-style-type: none"> (a) <i>the provision of the key information document by means of a website is appropriate in the context of the business conducted between the person advising on, or selling, a PRIIP and the retail investor;</i> (b) <i>the retail investor has been given the choice between information provided on paper and by means of a website and has chosen the latter in a way that can be evidenced;</i>
--	--	---

(c) the retail investor has been notified electronically, or in written form, of the address of the website, and the place on the website where the key information document can be accessed;

(d) the key information document remains accessible on the website, capable of being downloaded and stored in a durable medium, for such period of time as the retail investor may need to consult it.

Where the key information document has been revised in accordance with Article 10, previous versions shall also be provided on request of the retail investor.

6. For the purposes of paragraphs 4 and 5, the provision of information using a durable medium other than paper or by means of a website shall be regarded as appropriate in the context of the business conducted between the person advising on or selling a PRIIP and the retail investor if there is evidence that the retail investor has regular access to the internet. The provision by the retail investor of an email address for the purposes of that business shall be regarded as such evidence.

Furthermore, some Member States have been or are gold plating the EU consumer protection and financial market regulations. This makes it difficult from providers from other member states to offer their products and service. Hence, hindering the entrance of new players'; reserving the market for the domestic providers.

Please see below some example of national legislation that are an obstacle to the digitalisation of certain products and services:

◆ **In France:**

- **Contractualisation:** The rules governing the remote selling and canvassing of financial services are not harmonized, contrary to what has been done for other sectors with the Hamon Law, transposing the Directive 2011/83/EU on consumer rights resulting in the merger of the legal regimes of so-called direct marketing and distance selling.

In the financial sector, it is therefore necessary to apply two regulations instead of one, with provisions that are not completely identical. This does not facilitate the implementation of multichannel customer paths.

- **Execution of the contract:** The electronic writing is still discriminated against the written paper (according to article 314-26 of the RGAMF, a formal option from the customer is need for electronic communications. This article could be adapted.

The provisions of the Monetary and Financial Code on the account agreement (resulting from the transposition of the Payment Service Directive) distinguish the information provided by and the information provided to the customer. In order to prevent information relating to banking transactions (which need to be secured) from being sent to public e-mail addresses, or that the customer is saturated with SMS alerts notifying him of mails linked to the execution of the contract, contractual relations would be simplified by introducing a possibility, as in the case of account statements, that information relating to the execution of contracts could be provided or made available to the customer.

Ordonnance No. 2017-1433 of October 4, 2017 on the dematerialization of contractual relations in the financial sector (JO of 05/10/17) which has just been signed also discriminates the electronic writing of the paper: for the exercise of the right to open an account under the Payment Accounts Directive (PAD), which must be made in paper form, for the operations carried out in the context of direct marketing.

◆ **In Spain:**

The rules governing disclosure and transparency of information in case of mortgage lending are an obstacle to digitalization. For instance, when subscribing a mortgage loan that includes limitations on the variability of the interest rate (floor and ceiling clauses) or that involve the subscription of an interest rate risk hedging instrument, or that are granted in one or more currencies, the public deed shall be required to include, together with the client's signature, a handwritten expression by which the borrower declares that he or she has been adequately warned of the possible risks arising from the loan.

Another example is the requirement by Spanish laws of a physical signature before a notary for a mortgage to become enforceable. This means that only part of the experience can be digital, but the end should be done in a specific place (the notary's office). We believe there should be merit on integrating the digital public faith for these purposes.

		In terms of data protection, we believe that the GDPR is a major step forward. Any additional regulations on this subject would be counterproductive at this stage.
LOW LEVELS OF FINANCIAL LITERACY		
17	Are the issues identified by the EBA and the way forward proposed in subsection 4.4.5 relevant and complete? If not, please explain why.	<p>The European Banking Federation welcomes the proposed way forward suggested by the European Banking Authority to continue to foster national initiatives on financial literacy. It will contribute to strengthen the importance of developing and implementing financial education programs at national level. This should specifically include public authorities, as these are issues that go far beyond the framework of a mere banking relationship.</p> <p>Digital literacy and skills in particular call for a horizontal approach with public-private partnership and cross-sectoral cooperation, along with cooperation between various authorities.</p> <p>We believe that further joint action is needed by public authorities and relevant private stakeholders to help consumers make the best use of digital financial services, expanding awareness and empowering individuals with financial and digital skills. Policies to improve financial/digital literacy and help customers better understand the benefits and risks that they assume when using these new services should be targeted at individuals as well as any company that offers these types of services. Special emphasis should be attributed to financial/digital literacy in connection to the overall cybersecurity resilience and the ongoing digital fraud, with which all levels of society are daily confronted.</p>
18	Would you see the merit in having specific financial literacy programmes targeting consumers to enhance trust in digital services?	<p>Alongside with prudential regulation, both consumer protection and financial literacy are critical and complementary elements in ensuring a safe and sound financial system. Therefore, we believe that further joint action is needed by public authorities and relevant private stakeholders to help consumers make the best use of digital financial services, expanding awareness and empowering individuals with financial and digital skills.</p> <p>Cross-sectoral coordination of all interested stakeholders is thus essential when designing and implementing financial education initiatives. These should encompass all relevant public authorities (governments, central banks, financial authorities, bank supervisors, etc.), but their actions should be mindful not to substitute or duplicate existing efficient initiatives by private parties.</p>

We would like to stress the EBF example. We believe young people need to learn at an early stage how to manage their finances if they want to be successful in life. To promote the benefits of financial education and to raise awareness the EBF, together with its members, organises every year the **European Money Week** (EMW) an annual initiative involving more than 20 countries to discuss and learn about different experiences and views on financial education, promoting far-reaching financial education in Europe. It is worth noting that, as of next year, digital skills (especially in relation with cybersecurity) will become part of this initiative. The EBF remains ready to provide more information about this initiative to the EBA.

FINANCIAL EXCLUSION ASSOCIATED WITH ARTIFICIAL INTELLIGENCE AND DATA-DRIVEN ALGORITHMS

19	<p>Are the issues identified by the EBA and the way forward proposed in subsection 4.4.6 relevant and complete? If not, please explain why.</p>	<p>Data are at the centre of the digital revolution and consequently the use of data analytics is creating increasingly 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 businesses. Data analytics contribute widely to a better internal understanding of the banks' activities, a more effective risk management, and an improved monitoring of compliance. They can also contribute to building a stimulating customer experience.</p> <p>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.</p> <p>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:</p>
----	---	--

- **By enabling greater financial inclusion and simplifying the investment process for mass market:** It is expected that robo-advice's 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 contextualized, 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.

Websites, often run by startups, 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. Although the characteristics of “automated financial advice” limit human intervention, an access to an operator (via online chat, mail or telephone) may be provided to help the customer along the process. This issue is very important in particular where customer’s financial or digital knowledge is low. 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

		<p>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.</p> <p>Regarding possible malfunctioning of the tools due to errors, hacking or manipulation of the algorithm, it is important to emphasize the stringent cybersecurity regimes that banks follow, which protects the customer from this kind of manipulation and hacking. However, hacking or manipulation can occur in all type of entities. Therefore, it is important to monitor cybersecurity functions for all market participants in the same way and to maintain a true level playing-field.</p> <p>As a conclusion, the EBF strongly believes Big Data and Artificial Intelligence are technologies with a great potential to expand further the access to financial services through the lowering of the complexity and costs associated with some services (e.g. advisory and credit scoring services). We thus support the proposed way forward, with the note that, the concerns regarding the use of Big Data, prescriptive analysis, etc. will be handled adequately by the General Data Protection Regulation and the guidelines produced by the Article 29 Data Protection Working Party.</p>
--	--	---

THE IMPACT OF FINTECH ON THE RESOLUTION OF FINANCIAL FIRMS

20	<p>Are the issues identified by the EBA and the way forward proposed in section 4.5 relevant and complete? If not, please explain why.</p>	<p>With respect to the consequences of FinTech solutions implemented and used by banks the EBA has raised relevant issues. We note that continuing work on resolution of banks with regard to FinTech solutions should build on the Financial Stability Board (FSB)'s Key Attributes of Effective Resolution Regimes for Financial Institutions, updated 15 October 2014 and its subsequent related policy recommendations:</p> <ul style="list-style-type: none"> ▪ Guidance on Continuity of Access to Financial Market Infrastructures (FMIs) for a Firm in Resolution ▪ Guidance on Arrangements to Support Operational Continuity in Resolution ▪ Guidance on Identification of Critical Functions and Critical Shared Services <p>As well as the respective implementation of these recommendation in the European Bank Recovery and Resolution Directive and the Single Resolution Mechanism Regulation.</p>
----	--	--

Regarding the consequences of FinTech solutions implemented and used by the new FinTech firms not licenced as banks, the EBA may assess the questions of systemic and idiosyncratic risks posed by unregulated FinTechs.

So far resolution-related requirements on FinTech firms are not common and there are divergent practices emerging across jurisdictions in respect of the requirements for FinTech firms to have a resolution/recovery plan.

Generally, the EBF sees it as imperative to apply a prudential supervision, recovery and resolution framework and deposit insurance scheme such as provided for banks in the CRR, BRRD and DGSD – i.e. same risks / same activity needs to be regulated in the same manner. If the regulations of all FinTech companies are conducted on a basis of a level playing field, (the 4th guiding principles) then it will not be necessary to establish new resolution-setups. If a regulated FinTech-company goes into a partnership with a lawfully non-regulated FinTech, the present regulation regarding outsourcing will also handle the aspects of resolution of the activities of the non-regulated FinTech.

Where a FinTech resembles more central counterparty clearing financial institution the work going forward should build on the FSB's Guidance on Central Counterparty Resolution and Resolution Planning.

Policymakers should furthermore consider the following questions:

- How can a "resolution situation" in one or more FinTechs deteriorate the public's confidence in the regulated part of the financial sector ?
- How should "deposits" that clients of FinTech companies (e.g. payment service solutions) for shorter or longer periods hold by such companies be treated when it comes to the question of deposit guarantees? (as currently, they are not guaranteed) or are there any relevant arguments for including such firms in a Deposit Guarantee Scheme (DGS), e.g. a separate FDGS ("FinTech DGS")?
- How will the development of crowdfunding influence systemic risk and resolution?

THE IMPACT OF FINTECH ON AML/CFT

21	Do you agree with the issues identified by the EBA and the way forward proposed in section 4.6? Are there any other issues you think the EBA should consider?	<p>We feel the EBA addresses the correct risks in paragraph 4.6, but this could be more elaborated.</p> <p>Differences between AML/CFT regulatory regimes within EU Member States are only one of the risks regarding cross border services of FinTechs. Differences in regulatory approach on national and EU level, between traditional financial institutions and FinTechs, with regards to AML/CFT requirements are (just like the risks with regards to the prudential requirements as highlighted by the ECB) a serious risk.</p> <p>The same activities, same services, same risk, same rules, same supervision should apply. It is essential that the EU's AML/CFT framework does not distinguish between FinTechs - operating from the so called sandbox or innovation hub environments- and non-FinTech firms, like for regular financial institutions.</p> <p>Allowing new players to rely on AML/CFT requirements of traditional financial institutions such as Customer Due Diligence (CDD), data collection and transaction monitoring without having them to perform these duties on their own account, should be avoided.</p>
22	What do you think are the biggest money laundering and terrorist financing risks associated with FinTech firms? Please explain why.	<p>It is very difficult to give a single answer, because it depends on the product. The main risk is the new products in development that do not take into account AML risks.</p> <p>In our opinion, virtual currencies constitute a high risk with respect to money laundering and terrorist financing despite the fact that certain services and tools are being offered to mitigate those risks.</p> <p>In addition, as the FATF mentioned recently, the greatest risks of FinTech are often the lack of oversight or governance and the anonymity they can provide. In this respect, it is worrying that the counterpart of a payment through a PSP or FinTech is often not known by a bank. So, the bank cannot verify the name against sanction lists or assess the AML/CTF risk.</p>

<p>23</p>	<p>Are there any obstacles present in your national AML/CFT legislation which would prevent (a) FinTech firms from entering the market, and (b) FinTech solutions to be used by obliged entities in their customer due diligence process? Please explain.</p>	<p>The differences in the transposition in the Anti-Money Laundering Directive by Member States has hampered the ability of financial institutions to carry out customer identification and verification remotely and through digital means. This could not only be an obstacle for start-ups or new entrants on the market but also for the set-up of a harmonised European digital identity framework.</p> <p>For instance, the Spanish Regulation allows non-face-to-face identification by means of videoconference, while other Member States do not permit this. As a result, financial institutions in these Member States can initiate distant banking relationships (including cross-border) whereas other financial institutions are prevented from doing so in their own jurisdictions due to face-to-face identification still being required.</p> <p>The industry recognises that technology raises risks in AML/CTF compliance. However, we believe the benefits that technology can bring to this area exceed the risks. Automation and technology solutions to AML/CTF compliance as well as to other areas of regulatory reporting and monitoring have the potential to make processes more efficient and effective for both regulators and firms.</p> <p>We believe there is an urgent need to ensure coordination across regulatory bodies, particularly between financial regulators and data protection authorities. This is necessary to control for risk, but also to ensure that firms are enabled to bring forward technology enabled innovation which, as identified, will increasingly touch on regulations outside of the traditional scope of financial services regulators.</p> <p>As mentioned above in our response, the principle of “same services/activities, same risks, same rules and same supervision” should always be applied in order to ensure consumer protection and market integrity.</p>
-----------	---	--

About 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.

www.ebf.eu @EBFeu

For more information contact:

Noémie Papp
Head of Digital & Retail
n.papp@ebf.eu
+32 2 508 37 69

About 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.

www.ebf.eu @EBFeu

For more information contact:

Noémie Papp
Head of Digital & Retail
n.papp@ebf.eu
+32 2 508 37 69