Contribution ID: c54d07b2-127e-47c8-a214-8af203471614
Date: 26/06/2020 19:41:31

Consultation on a new digital finance strategy for Europe / FinTech action plan

Fields marked with * are mandatory.

Introduction

This consultation is now available in 23 European Union official languages.

Please use the language selector at the top of this page to choose your language for this consultation.

1. Background for this consultation

Digitalisation is transforming the European financial system and the provision of financial services to Europe's businesses and citizens. In the past years, the EU and the Commission embraced digitalisation and innovation in the financial sector through a combination of horizontal policies mainly implemented under the umbrella of the Digital Single Market Strategy, the Cyber Strategy and the Data economy and sectoral initiatives such as the revised Payment Services Directive, the recent political agreement on the crowdfunding regulation and the FinTech Action Plan. The initiatives set out in the FinTech Action Plan aimed in particular at supporting the scaling up of innovative services and businesses across the EU, for example through enhanced supervisory convergence to promote the uptake of new technologies by the financial industry (e.g. cloud computing) but also to enhance the security and resilience of the financial sector. All actions in the Plan have been completed.

The financial ecosystem is continuously evolving, with technologies moving from experimentation to pilot testing and deployment stage (e.g. blockchain; artificial intelligence; Internet of Things) and new market players entering the financial sector either directly or through partnering with the incumbent financial institutions. In this fast-moving environment, the Commission should ensure that European consumers and the financial industry can reap the potential of the digital transformation while mitigating the new risks digital finance may bring. The expert group on Regulatory Obstacles to Financial Innovation, established under the 2018 FinTech Action Plan, highlight these challenges in its report published in December 2019.

The Commission's immediate political focus is on the task of fighting the coronavirus health emergency, including its economic and social consequences. On the economic side, the European financial sector has to cope with this unprecedented crisis, providing liquidity to businesses, workers and consumers impacted by a sudden drop of activity and revenues. Banks must be able to reschedule credits rapidly, through rapid and effective processes carried out fully remotely. Other financial services providers will have to play their role in the same way in the coming weeks.

Digital finance can contribute in a number of ways to tackle the COVID-19 outbreak and its consequences for citizens, businesses, and the economy at large. Indeed, digitalisation of the financial sector can be expected to accelerate as a consequence of the pandemic. The coronavirus emergency has underscored the importance of innovations in digital financial products services, including for those who are not digital native, as during the lockdown everybody is obliged to rely on remote services. At the same time, as people have access to their bank accounts and other financial services remotely, and as financial sector employees work remotely, the digital operational resilience of the financial sector has becoming even more important.

As set out in the Commission Work Programme, given the broad and fundamental nature of the challenges ahead for the financial sector, the Commission will propose in Q3 2020 a new Digital Finance Strategy/FinTech Action Plan that sets out a number of areas that public policy should focus on in the coming five years. It will also include policy measures organised under these priorities. The Commission may also add other measures in light of market developments and in coordination with other horizontal Commission initiatives already announced to further support the digital transformation of the European economy, including new policies and strategies on data, artificial intelligence, platforms and cybersecurity.

2. Responding to this consultation and follow up

Building on the work carried out in the context of the FinTech Action Plan (e.g. the EU Fintech Lab), the work of the European Supervisory Authorities and the report issued in December 2019 by the Regulatory Obstacles to Financial Innovation Expert Group, and taking into account the contribution digital finance can make to deal with the COVID-19 outbreak and its consequences, the Commission has identified the following four priority areas to spur the development of digital finance in the EU:

1. ensuring that the EU financial services regulatory framework is fit for the digital age;
2. enabling consumers and firms to reap the opportunities offered by the EU-wide Single Market for digital financial services;
3. promoting a data-driven financial sector for the benefit of EU consumers and firms; and
4. enhancing the digital operational resilience of the EU financial system.

In this context and in line with Better Regulation principles, the Commission is launching a consultation designed to gather stakeholders' views on policies to support digital finance. It follows two public consultations launched in December 2019, focusing specifically on crypto-assets and digital operational resilience.

This consultation is structured in three sections corresponding to the priorities areas 1, 2 and 3 presented above. Given that the ongoing consultation on digital operational resilience fully addresses the issues identified as part of this priority area, questions on this priority area are not reproduced in this consultation. As for priority area 1, this consultation includes additional questions given that this priority area goes beyond the issues raised in the currently ongoing consultation on crypto-assets. In addition, the Commission will also be consulting specifically on payment services. Payment services and associated technologies and business models are highly relevant for the digital financial fabric, but also present specificities meriting separate consideration. These considerations are addressed in a specific consultation on a Retail Payments Strategy launched on the same day as this one. Finally, and specific to financial services, the Commission is also supporting the work of a High Level Forum on Capital Markets Union, that is expected to also address key technology, business model and policy challenges emerging from digitalisation.

The first section of the consultation seeks views on how to ensure that the financial services regulatory framework is technology neutral and innovation-friendly, hence addressing risks in a proportionate way so as not to unduly hinder the emergence and scaling up of new technologies and innovative business models while maintaining a sufficiently cautious approach as regards consumer protection. While an in-depth assessment is already on-going on

crypto-assets, assessment of whether the EU regulatory framework can accommodate other types of new digital technology driven services and business models is needed. Looking at a potentially more complex financial ecosystem - including a wider range of firms, such as incumbent financial institutions, start-ups or technology companies like BigTechs - the Commission is also seeking stakeholders' views on potential challenges or risks that would need to be addressed.

The second section invites stakeholder views on ways to remove fragmentation of the Single Market for digital financial services. Building on the preparatory work carried out in the context of the 2018 FinTech Action Plan, the Commission has already identified a number of obstacles to the Single Market for digital financial services and is therefore seeking stakeholders' views on how best to address these. In addition, the consultation includes a number of forward-looking questions aiming to get stakeholders' feedback as regards other potential issues that may limit the deepening of the Digital Single Market and should be tackled at EU level.

Finally, the third section seeks views on how best to promote a well-regulated data-driven financial sector, building on the current horizontal frameworks governing data (e.g. General Data Protection Regulation; Free Flow of Data Regulation) but also on the recent sectoral developments such as the implementation of the revised Payment Services Directive in the EU. Considering the significant benefits data-driven innovation can bring in the EU across all sectors, the Commission recently adopted a new European Data Strategy and a White Paper on Artificial Intelligence. Building on these horizontal measures, the Commission is now seeking stakeholders' views on the potential additional measures that would be needed in the financial sector to reap the full benefits of the data economy while respecting European values and standards. Responses to this consultation will inform forthcoming work on a Digital Finance Strategy/FinTech Action Plan to be adopted later in 2020.

Please note: In order to ensure a fair and transparent consultation process **only responses received through our online questionnaire will be taken into account** and included in the report summarising the responses. Should you have a problem completing this questionnaire or if you require particular assistance, please contact fisma-digital-finance@ec.europa.eu.

More information:

- on this consultation
- on the consultation document
- on digital finance
- on the protection of personal data regime for this consultation

About you

* Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish
-

- Dutch
- (•) English
- Estonian
- Finnish
- French
- Gaelic
- German
- Greek
- Hungarian
- Italian
- Latvian
- Lithuanian
- Maltese
- Polish
- Portuguese
- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as

- Academic/research institution
- (•) Business association
- Company/business organisation
- Consumer organisation
- EU citizen
- Environmental organisation
- Non-EU citizen
- Non-governmental organisation (NGO)
- Public authority
- Trade union
- Other

* First name

Liga

* Surname

Semane

* Email (this won't be published)

l.semane@ebf.eu

* Organisation name

255 character(s) maximum

European Banking Federation

* Organisation size

- ○ Micro (1 to 9 employees)
- ◉ Small (10 to 49 employees)
- ○ Medium (50 to 249 employees)
- ○ Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

4722660838-23

* Country of origin

Please add your country of origin, or that of your organisation.

- ○ Afghanistan
- ○ Åland Islands
- ○ Albania
- ○ Algeria
- ○ American Samoa
- ○ Andorra
- ○ Djibouti
- ○ Dominica
- ○ Dominican Republic
- ○ Ecuador
- ○ Egypt
- ○ El Salvador
- ○ Libya
- ○ Liechtenstein
- ○ Lithuania
- ○ Luxembourg
- ○ Macau
- ○ Madagascar
- ○ Saint Martin
- ○ Saint Pierre and Miquelon
- ○ Saint Vincent and the Grenadines
- ○ Samoa
- ○ San Marino
- ○ São Tomé and Príncipe

- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Guadeloupe
- Guam
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar /Burma
- Namibia
- Nauru
- Nepal
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Syria

- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay

- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cuba
- Curaçao
- Cyprus
- Czechia
- Democratic Republic of the Congo
- Denmark
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Liberia
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Rwanda
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Saint Kitts and Nevis
- Saint Lucia
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara
- Yemen
- Zambia
- Zimbabwe

* Field of activity or sector (if applicable):

at least 1 choice(s)

- [ ] Accounting
- [ ] Auditing
- [x] Banking
- [ ] Credit rating agencies
- [ ] Insurance
- [ ] Pension provision
- [ ] Investment management (e.g. hedge funds, private equity funds, venture capital funds, money market funds, securities)
- [ ] Market infrastructure operation (e.g. CCPs, CSDs, Stock exchanges)
- [ ] Technology companies
- [ ] Organisation representing European consumers' interests
- [ ]

Organisation representing European retail investors' interests

- ☐ National supervisory authority
- ☐ European supervisory authority
- ☐ Other
- ☐ Not applicable

* Publication privacy settings

The Commission will publish the responses to this consultation. You can choose whether you would like your details to be made public or to remain anonymous.

- ○ **Anonymous**
  Only your type of respondent, country of origin and contribution will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.
- ◉ **Public**
  Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

☑ I agree with the personal data protection provisions

General questions

Europe's strategic objective should be to ensure that European consumers and firms fully reap the benefits stemming from digital finance while being adequately protected from the potential new risks it may bring. To achieve that, the European financial sector needs to be at the forefront of innovation and its implementation in a market and production environment in order to better serve consumers and firms in an efficient, safe, sound and sustainable manner. Strong and innovative digital capacities in the financial sector will help improve the EU's ability to deal with emergencies such as the COVID-19 outbreak. It will help to further deepen the Banking Union and the Capital Markets Union and thereby strengthen Europe's economic and monetary union and to mobilise funding in support of key policy priorities such as the Green Deal and sustainable finance. It is also essential for Europe to safeguard its strategic sovereignty in financial services, and our capacity to manage, regulate and supervise the financial system in a way that promotes and protects Europe's values and financial stability. This will also help to strengthen the international role of the euro.

With a view to adopt a new Digital Finance Strategy/FinTech Action Plan for Europe later this year, the Commission is now seeking your views to identify the priority areas for action and the possible policy measures.

Question 1. What are the main obstacles to fully reap the opportunities of innovative technologies in the European financial sector (please mention no more than 4)?

Please also take into account the analysis of the expert group on Regulatory Obstacles to Financial Innovation in that respect.

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The EBF support the recommendations made in the ROFIEG report. We would like to highlight the following obstacles which prevent banks from fully taking advantage of the opportunities offered by innovative technologies in the financial sector:

1. Fragmentation across Europe due to diverging regulatory frameworks adopted by national competent authorities affects the level playing field for providers of the same services, creates asymmetries between member states and imposes additional costs for compliance with multiple regimes. Some examples are: the process of opening a bank account, which can be very different between member countries namely due to diverging AML/CFT related requirements; obstacles to the adoption of cloud computing due to gold plating following the EBA Guidelines on outsourcing; and constraints in the adoption of AI due to a lack of clarity on how existing requirements apply to new AI use cases.

2. Regulation should be principle-based, to ensure that requirements are fit for digital innovation. The more detailed the regulatory requirements are, the more difficult it becomes for the financial sector to innovate. Legislation should also be flexible enough to allow the requirements to remain relevant even though different technologies are constantly developing.

3. The banking sector operates with specific, stricter requirements (prudential, consumer protection, corporate governance, etc.) which other market players are not subject to due to their categorization as "non-banking institutions" although they provide multiple services provided by banks. This does not favour fair competition in the context of the provision of digital services to consumers within the financial sector between different players. It also results in banks facing slower time-to market for new products due to stricter governance procedures and requirements, which, in addition to affecting competition, hampers innovation. This makes the principle of "same services, same risks, same rules and same supervision" crucial.

The implications of the consolidated application of prudential rules to banking groups, which leaves digital subsidiaries of banking groups in a situation of competitive disadvantage versus other players, is discussed under Recommendation 13 of the ROFIEG Report. Not only belonging to a bank group automatically attracts all prudential requirements for all the subsidiaries, but also, the way proportionality applies limits the capacity to adapt the governance framework of a subsidiary to the actual activity it performs and the risks it creates.

4. Existing asymmetries as regards rules on access to data - Recommendations 27 and 28 of the ROFIEG Report. In particular, PSD2 obliges banks to allow users to share payments data with third parties, including via APIs (application programming interfaces). This creates an asymmetry in access to data, as non-bank players do not have similar requirements to make their own core customer data (which typically differs from payments) shareable with third parties, including banks. This puts the financial sector at a disadvantage when competing in digital markets. Future EU initiatives on data sharing, such as those outlined in the Commission's Data Strategy, must have a focus on cross-sectoral data sharing and empowering users – individuals and firms. More broadly, there is also a need to reconcile the regulation of personal and non-personal data with the opportunities offered by FinTech.

Additional obstacles we would like to flag are:

- A lack of education with a focus on digitalisation capabilities.
- Fair access to infrastructure and platforms. Competition policy and existing regulation might be insufficient to ensure fair and even competitive conditions in digital markets in which large platforms benefit from network effects and gatekeeping roles. A particular issue hampering the level playing field in financial services is the lack of access, under fair conditions, to some technical infrastructure needed for the provision of financial services. The importance of addressing the latter has also been highlighted in the ROFIEG

Report (Recommendation 22). Infrastructure hosts have the power to build ecosystems in which the user is locked-in and any third-party provider is dependent on the increasingly demanding conditions that the hosts may decide to impose. Digital infrastructures with critical mass of users should be required to give access to third-party providers under fair, transparent, and objective conditions.

Question 2. What are the key advantages and challenges consumers are facing with the increasing digitalisation of the financial sector (please mention no more than 4)?

For each of them, what if any are the initiatives that should be taken at EU level?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In the increasing digitalisation of the financial sector, and with the view to guarantee a sound and overarching protection of consumers, we recall that it is crucial for regulation to target services and products, not providers. For this purpose, the principle “same services, same risk, same rules, same supervision” should be applied not only by banks but also by non-bank providers.
The COVID-19 crises made digital services increasingly necessary. EBF members have seen a seen a rapid adaptation from consumers given the situation. An assessment will be needed to determine how much of these changes will stay and how the need for physical interaction has changed, to accommodate to customers’ needs.

Advantages:

- Greater efficiency in processes, both in client oriented (e.g. electronic signature, creation of banking applications for the smartphone, improving customer on-boarding processes and making transactions more transparent, efficient, and more secure through various technologies) and internal processes (e.g. through the adoption of cloud computing technology in the financial sector).
- An improved user experience and more choices between products and services. Digitalisation has also improved the facility of switching providers, as this can be done digitally.
- Increased transparency for customers resulting from the greater ease of comparison between offers.
- Increased control of and engagement with, the management of finances
- Technologies such as big data and AI give the opportunity to improve services for customers (e.g. innovative credit scoring and better product segmentation and development through the use of big data).

Challenges:

- Trust in digital offers, due to data protection and security concerns. On the latter, scamming, phishing, and hacker attacks are examples of potential threats to consumers. They may suffer losses or other detriment in the event of a cybersecurity incident or fraud.
- A consumer protection risk due do a difficulty in understanding new financial developments (e.g. crypto assets) and a lack of awareness of the regulatory status of new players (and associated protections), exacerbated by digital literacy and technology. This can affect the confidence of consumers, which is a key value in the financial sector. Consumers need to be able to differentiate providers that are ruled by strict supervisory rules from providers that are subject to lighter requirements - and hence often less due diligence and compliance controls. Fragmentation and complexities, for example, from the types of payments and the

liabilities associated with that, such as fraud.

- Complex identification processes due to extensive variation in technical definitions and required identification processes between member states. Extended Due Diligence requirements have been imposed to comply with KYC/AML regulation at national level, adding more complexity and effort to the process. A lack of clear and consistent guidance to support firms with remote onboarding for consumers, including on e-signatures and e-ID, is undermining the development of interoperability and common standards.
- Risk of digital and/or financial exclusion. Consumer risks may be exacerbated where customer face digital literacy problems or where technology might act as a barrier to access key financial services. Action in financial education is therefore essential.

Possible solutions are:

- Use of regulatory sandboxes.
- Widening the regulatory perimeter in line with the principle 'same activity, same risk, same regulation'
- Supporting initiatives on financial and digital education. See Questions 24-45 for further comments.

Building on previous policy and legislative work, and taking into account the contribution digital finance can make to deal with the COVID-19 emergency and its consequences, the Commission services are considering four key priority areas for policy action to spur the development of digital finance:

1. ensuring that the EU financial services regulatory framework is technology-neutral and innovation friendly;
2. reaping the opportunities offered by the EU-wide Single Market for digital financial services for consumers and firms;
3. promoting a data-driven financial sector for the benefit of EU consumers and firms; and
4. enhancing the operational resilience of the financial sector.

Question 3. Do you agree with the choice of these priority areas?

- (●) Yes
- ( ) No
- ( ) Don't know / no opinion / not relevant

Question 3.1 Please explain your answer to question 3 and specify if you see other areas that would merit further attention from the Commission:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Priority 1: We fully support the efforts towards the development of legislation that is horizontal and sufficiently flexible to protect all consumers irrespective of new technologies or products. European banks recommend a technologically neutral approach to provide clarity to the market regarding applicable requirements for digital innovation. Without such clarity, innovative services/functions will not be implemented by traditional market players. However, if policymakers are developing new frameworks, it is important to consider technology, otherwise the regulation may not be fully fit for purpose.
Also, while the focus of increasing technology adoption is important, it lacks the perspective of business model adoption. This makes the prudential perimeter a key issue, serving as a barrier to banks' further

adoption of digital business models. Ensuring a level playing field must be a key part of a technology-neutral, innovation friendly policy approach. Only by ensuring fair competition among players can the EU maximize the benefits of innovation in finance.
Priority 2: We agree with the Commission's view that market-fragmentation is one of the key challenges for developing financial services at scale in Europe. Divergent approaches also carry a risk of regulatory arbitrage and may create an unlevel playing field across countries, particularly as digitalisation increases the cross-border provision of financial services. Clear, simple, future-proof, and overarching rules are essential in order to guarantee consumer protection, and to embrace the digitalization of the financial market. Rules should be principles-based to leave room to adapt to technological evolution. We would also like to highlight the importance of, a globally consistent regulatory framework.

Priority 3 : We support the initiative to promote a data-driven financial sector as this contributes to building a European Data Economy. However, open data should be delivered on a cross-sectorial basis that is not specific to financial services. If a sectoral approach is taken, as proposed through Open Finance, members see an enormous risk of further unlevelling the playing field, where some firms, such as large digital platforms, act as data gatekeepers, potentially creating market oligopolies, and ultimately restricting innovation and choice for consumers. Establishing a cross sectoral data sharing framework, which ensures that customers are given the option to choose what data they wish to share and with whom and that they are given the tools to do so, should be the priority. Echoing the ROFIEG report, we do agree that firms may be held back due to uncertainties about how to comply with data protection rules when using blockchain, AI and certain other technologies. Clarification on the interaction of different regulations might be needed. Also in the field of data, we favour the development of a more streamlined process of accepting valid KYC. Please see the EBF AML Blueprint for further recommendations in this regard.

Priority 4: Cloud and ICT providers in general have become key for banks to make the most of the digital promises. Considering existing SOC (System and Organisation Controls)2 reports – giving insights on operational effectiveness of agreed controls on third party providers – more standardization by certification could be helpful within the oversight framework. Beyond that, EU-level considerations of a specific oversight for TPPs, based on international coordination, should be risk-based and should target these providers without imposing additional requirements for banks. It is important to introduce the advancement of supervisory powers over TPPs horizontally across industry sectors, and not to limit the changes (neither explicitly nor de facto) to the financial sector. Horizontally applied, we see merit in the assessment of the CSPs due to qualitative and quantitative features (such as number of providers, market shares, risk-profile), establishing their critical status for the sector service provision. The criticality established by banks' service assessments for outsourcing can be a significant indicator for the criticality of the respective TPP. However, one should also keep in mind the possibilities of providers to engage within a 'supply chain', or potentially being used by banks' service providers within one chain as a "fourth party" (subcontracting constellations). The potential for concentration risk is thereby not limited to the bilateral engagement of providers and financial institutions, and we recommend the Commission to take a holistic view on the criticality of supply chains as well.

When doing so, any consideration of potentially direct oversight needs a thorough assessment of its potential implications as it may not only reduce compliance burdens for firms, but may have negative side effects, such as limited choice of suppliers for financial institutions.

I. Ensuring a technology-neutral and innovation friendly EU financial services regulatory framework

In order to be fit for the digital age, the EU financial services regulatory framework should neither prescribe nor prevent the use of particular technologies whilst ensuring that regulatory objectives continue to be satisfied. It should also not hinder the emergence and scaling up of innovative business models, including platform-based ones, provided that the new risks these new business models may bring are properly addressed. The Commission undertook an in-depth assessment of these issues in the context of the FinTech Action Plan and is already acting on certain issues. Even so, in this fast-moving and increasingly complex ecosystem, it is essential to monitor technological and market trends on a regular basis and to identify at an early stage whether new regulatory issues, including e.g. prudential ones, are emerging and, if so, how to address them in a proportionate manner.

Question 4. Do you consider the existing EU financial services regulatory framework to be technology neutral and innovation friendly?

- ○ Yes
- ◉ No
- ○ Don't know / no opinion / not relevant

Question 4.1 If not, please provide specific examples of provisions and requirements that are not technologically neutral or hinder innovation:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We recognize much effort has been invested by the Commission and other European authorities over the last years to embed the principle of technological neutrality in all relevant EU regulatory initiatives. The principle continues to be essential to respond to existing challenges. However, there are still issues in the EU financial regulatory framework that run to the principle:

- Prudential rules
  - (Lack of) application of proportionate prudential rules / consolidation hinder the uptake of technology by banks versus other players: Impact of prudential rules on digital subsidiaries of banking groups.
  - Prudential treatment of banks' investment in software under the Capital Requirements Regulation.
  - Banks' attraction of digital talent hindered by remuneration rules.
  - Increased time-to-market of banks digital transformation processes (e.g. by imposing internal control and risk management frameworks)

- PSD2
  - Sustainability issue with cost of developing and maintaining infrastructure, reducing capacity to invest.
  - Innovation: wrong incentives for development of new payment functionality, as future payments functionality must be opened up to third parties without any remuneration.
  - Strong Customer Authentication: the current requirements applied to certain forms of electronic payments, such as contactless transactions, can create a barrier to the development of innovative and user-friendly forms of payment.

- Payments
  - Regulation of the payments chain focuses on banks, e.g. Interchange Fee Regulation, reducing the incentives to innovate. On the contrary, non-regulated actors offering payment solutions such as some digital wallet providers are becoming dominant players in the market. This allows them to restrict the access to app stores or technical elements such as the Near Field Communication (NFC) antenna or biometric sensors,

impose fees that squeeze payment margins and even introduce non-negotiable clauses in their contracts that contradict financial regulation requirements. Differences in implementation of EU legislation, and differences in supervisory practices and priorities, combined with the ability of payment institutions and e-money institutions to passport across the EU, make for an opaque and fragmented situation where not all PI and EM institutions may be held to the same standards.

• Differences between level 1 and level 3 measures. In many cases, the level 1 legislation is technology-neutral, but many times has complementary level 3 measures, namely in the form of Opinions or Guidelines, with technical specifications that impact banks' development cycles and costs. For example, new guidelines which set specific requirements on the procedure to grant loans or the data to be used by financial institutions, such as the EBA Guidelines on loan origination and monitoring, might also end up hindering the use of AI by financial institutions, and increasing the gap with non-bank players not subject to this regulation.

• DLT based applications may raise jurisdictional issues about the applicable legislation and liability issues. The legal validity and enforceability of smart contracts may need some clarification. The EBF looks forward to the Commission to address this issue further. When looking at DLT applications, the principle of "same services, same risks, same rules" is important. The decentralized character of DLT provides challenges vis-à-vis the centralized approach under today's financial regulation for securities market and post-trade services. The challenge of changing relationship due to technology has also be identified by the ROFIEG report. We find some issues in the securities market regulatory framework, as some of those rules and requirements can be difficult to apply to decentralized DLT schemes. For instance, the strong regulation defining what a trading venue is and its obligations is technology agnostic but defines a centralized operation, notwithstanding the market fragmentation concept in place since 2007. While applying trading venue definitions and requirements can be easier to a centralized DLT trading venue, there can be uncertainty in the application of these concepts to a decentralized one. Even in a centralised scenario, issues regarding how DLT technology is to be applied will need further clarification, such as the status of each node, the non-discriminatory access to venues and how price formation is due to occur. Regarding post-trade services, at present, the legal framework for registry, clearing and settlement of securities defines a centralized operation of central securities depositories (CSDs), which is difficult to reconcile with decentralized DLT scenarios, which might also enable alternative mechanisms to mitigate counterparty risk different to the centralized system prescribed under EMIR.

Question 5. Do you consider that the current level of consumer protection for the retail financial products and services established by the EU regulatory framework is technology neutral and should be also applied to innovative ones using new technologies, although adapted to the features of these products and to the distribution models?

- (●) Yes
- ( ) No
- ( ) Don't know / no opinion / not relevant

Question 5.1 Please explain your reasoning on your answer to question 5, and where relevant explain the necessary adaptations:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that horizontal and sufficiently flexible technology-neutral regulation is key to ensure sound consumer protection in a continuously evolving digital market. More specifically, flexibility would allow legislation to remain relevant, adapt to the changes in technology and ensure consumer protection (also as the timing of the EU decision making process in terms of negotiations, implementation, etc. makes continuous adjustments of legislation in response to evolving technologies challenging). For example, we particularly praise the design of the Distance Marketing of Financial Services Directive, that by being principle-based rather than rule-based, was able to adapt to the evolving use of digital devices and continues ensuring a high level of consumer protection.
Some of the requirements provided by the current regulatory framework for financial products and services we deem important a certain level of harmonization with the needs of an increasingly digitalised market, such as:

- The PRIIPS document and PAD document fit the needs for physical, not digital interaction. Instead of following a specific format, the principle based approach should be followed. Another example is the current MiFID regulatory framework and the conditions applying to the provision of information. In practise the regulation means that service providers are asking large amounts of clients if they want to use web-based digital documents, but if an answer from a customer is not received, the papers still need to be printed and mailed. We propose that specific consent for the delivery of the information in a durable medium other than paper should not be a requirement. Thus, paper should not be the default option.
- Strong Customer Authentication (SCA) requirements have been developed taking into consideration “traditional” authentication processes involving two factors of different nature (knowledge, possession, inherence). Yet, this approach disregards the possibility that technology or procedures evolve in a way that SCA can be ensured just using one “robust” factor or two factors of the same nature, for instance.
- Responsibilities between third parties, FinTechs & banks. Particularly in payments, financial regulation designates banks as the single point of contact for users’ claims on transactions wrongly executed involving banks, FinTechs and/or other parties. Moreover, banks are the party ultimately responsible for SCA so that if a transaction is defectively authenticated, they have to bear any potential loss. Although these provisions are meant to guarantee users’ redress in unexpected situations, they also reduce the ability of banks to delegate these activities to take advantage of innovations provided by third parties or FinTechs involved in the transaction, and can create additional administrative burdens for banks when they must pursue other entities that are at fault in order to be compensated, particularly in the absence of clear dispute resolution frameworks.
- Suitability and application of EU regulatory framework in respect of consumer protection is often dependant on the type of regulated entity providing the financial service/product. For example, the EU Deposit Guarantee Schemes which compensates depositors in the event of a bank’s failure, is solely funded by banks (acting as deposit taking institution) and only covers eligible deposit products (which will not include many new Fin-Tech offerings). Given bank-like substitute consumer offerings through E-money Issuers and alternative Payment Institutions, the development of digital retail financial products and services should require clear and transparent messaging as to the level of prudential protection afforded to customer based on the product provider/product type. In addition, prudential protections such as DGS could be extended to such new offerings to mitigate prudential risk.

Overall, it is crucial to respect the principle of “same services, same risks, same rules and same supervision” in order to ensure consumer protection and level playing field. If the requirements are different, the customer will have different levels of protection depending on who provides the service, which the general public may not understand.

Finally, entities should also be able to analyse whether business models based on new technologies are viable. Below we highlight the role of the sandboxes or controlled test environments. However, it would also

be positive for consumers if regulated entities also had the opportunity to innovate at digital speed in a more permanent manner, for ongoing testing processes.

Identify areas where the financial services regulatory framework may need to be adapted

The use of Distributed Ledger Technology (DLT), and in particular the use of one of its applications, the so-called crypto-assets, have been identified as an area where the European regulatory framework may need to be adapted. A public consultation on crypto-assets is on-going to gather stakeholders' views on these issues. Beyond the area of crypto assets, and looking at other technological and market developments, the Commission considers that it is important to identify potential regulatory obstacles to innovation at an early stage and see how to best address these obstacles not to slow down the uptake of new technologies in the financial sector.

Question 6. In your opinion, is the use for financial services of the new technologies listed below limited due to obstacles stemming from the EU financial services regulatory framework or other EU level regulatory requirements that also apply to financial services providers?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N.A.
Distributed Ledger Technology (except crypto-assets)	○	○	○	◉	○	○
Cloud computing	○	○	○	○	◉	○
Artificial Intelligence/Machine learning	○	○	○	○	◉	○
Internet Of Things (IoT)	○	○	○	◉	○	○
Biometrics	○	○	○	◉	○	○
Quantum computing	○	○	○	◉	○	○
Other	○	○	○	◉	○	○

If you see other technologies whose use would be limited in the financial services due to obstacles stemming from the EU financial services legislative framework, please specify and explain:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Digital Identity encounters obstacles for true EU-wide usage due to a lack of operational standards, especially in the private sector which creates a lack of interoperability across borders. Furthermore, better access to data could help enhance the uptake of e-ID. The more data points available in an e-ID, the more secure and reliable electronic identification is. An EU wide framework for allowing cross-sectoral data sharing in a safe and highly regulated environment could improve the effectiveness and reliability of e-ID solutions. This type of data sharing should be subject to the data subject's explicit consent and the GDPR's overarching safeguards. Clear rules on the handling and storage of biometric data could also help the uptake of e-ID.

Question 6.1 Please explain your answer to question 6, specify the specific provisions and legislation you are referring to and indicate your views on how it should be addressed:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

• DLT: Fragmentation of rules for inherently cross-border focused technology across the EU would limit growth of DLT applications. A pan-European approach, targeting a technological neutrality of rules while applying the principle “same services, same risks, same rules”, needs be defined to avoid potential divergences that different national legislative initiatives could introduce. Legal clarity on questions such as the character of smart contracts and the interaction with rights under the GDPR (e.g. data deletion) will be central to the options for adoption of DLT in the financial industry. We refer to recommendation 6 of the ROFIEG report, which sets out the regulatory regimes that will need to be considered in a DLT environment. In respect of crypto-assets a first step should be establishing a clear and precise taxonomy that differentiates different crypto-asset categories to enable proper regulation and supervision according to their characteristics and risks. This could also take into account defining and understand key technical features of DLT. There should be neither detrimental regulatory fragmentation nor grey zones with insufficient consumer and investor protection. This means that besides legal classification of technological features, such as smart contracts, it is important to cover new market entrants in financial services (e.g. wallet providers and service validators) under the same rules that provide consumer/investor protection today.
• Cloud computing: Following the 2019 EBA Guidelines (GL) on outsourcing, it is important to avoid fragmentation of the supervisory framework for cloud solutions by diverging implementation in Europe. For example, in some countries financial institutions need to have prior, explicit authorization to outsource a particular service to the cloud, while in some other jurisdictions a notification is sufficient. Such fragmentation creates regulatory uncertainty, ultimately holding banks back in cloud adoption. A clear understanding of supervisory rules, coherent for the inherent cross-border nature of cloud computing, is key to enable banks’ cautious and gradual approach to utilize cloud services safely under the strict financial regulatory framework. A common and coordinated supervisory approach is required to enable financial institutions to develop consistent approaches in all jurisdictions where they operate and benefit from the potential of cloud as other industries do. Complementing the harmonized supervisory implementation of the

EBA GL, financial institutions will benefit from the Commission's upcoming voluntary standard contractual clauses on cloud, addressing potential asymmetries in the negotiation between institutions and providers. The EBF encourages the Commission in their strive for market impact of this helpful guidance.

- AI: AI offers new opportunities to improve the accuracy of risk models. Yet, the regulatory framework for the approval of regulatory models is demanding, and bank's experience of implementing changes in the model development methodologies is costly, involving approval times which, in some cases, can be very extensive. More clarity on how the current regulatory framework will be applied when using AI, e.g. regarding how the approval process will work in practice with AI models (in terms of timing, involved teams, assessment of material changes, etc.) would be welcome. Uncertainties as regards GDPR and AI developments are also a challenge (see Question 37 for further details).
- Biometrics: as with other remote identity technologies, harmonization is needed regarding the acceptable use of biometrics across the EU. In addition, many biometric tools are embedded in third party devices, and therefore subject to ICT risk management requirements which do not apply to non-bank competitors which are not subject to this rules.

Other pieces of the financial regulatory framework which create challenges include software deductions from CET1 and remuneration policies create a competitive disadvantages when hiring.

Measures that can facilitate the uptake of technologies in finance include:

- Wide use of regulatory sandboxes would help to rapidly understand new technologies and their applications, also by regulators/ supervisors.
- Avoiding prescriptive criteria in regulation. Building in flexibility will also allow to take into account the variety and rapidly evolving nature of new technologies, such as AI.
- Mitigating the negative implications of prudential regulation/supervision.
- One-stop-shop approach to supervision/regulation.
- Avoiding fragmentation across member states through harmonized legislation and application, which would facilitate a faster and sounder scalability of solutions. E.g. on crypto-assets, cloud, AI, and biometrics.
- Providing guidance on how to observe existing requirements and supervisory expectations rather than developing specific rules
- Adopting a globally consistent approach.

Question 7. Building on your experience, what are the best ways (regulatory and non-regulatory measures) for the EU to support the uptake of nascent technologies and business models relying on them while also mitigating the risks they may pose?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N.A.
Setting up dedicated observatories to monitor technological and market trends (e.g. EU Blockchain Observatory & Forum; Platform Observatory)	○	○	○	◉	○	○

Funding experimentation on certain applications of new technologies in finance (e.g blockchain use cases)	○	○	○	◉	○	○
Promoting supervisory innovation hubs and sandboxes	○	○	○	○	◉	○
Supporting industry codes of conduct on certain applications of new technologies in finance	○	○	○	◉	○	○
Enhancing legal clarity through guidance at EU level for specific technologies and/or use cases	○	○	○	○	◉	○
Creating bespoke EU regimes adapted to nascent markets, possibly on a temporary basis	○	○	◉	○	○	○
Other	○	○	○	◉	○	○

Please specify what are the other ways the EU could support the uptake of nascent technologies and business models relying on them while also mitigating the risks they may pose:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

"Other" item:

- Increased cooperation between European Supervisory Authorities and National Competent authorities for better coordination on new technologies (e.g. AI). As the relevant topics go beyond the financial sector, there is a need to involve, for example, data protection authorities as well. A cross- sectoral sandbox regulatory could be explored.
- The creation of sandboxes for financial institutions to test new ideas and technologies on a trial-basis, with the support of the relevant authorities, so that the minimum viable product (MVP) can be proved and more fit for purpose regulation can be adopted.
- The organisation of EU-wide hackathons focused on different challenges and to dedicate research funding into technology readiness levels.
- Industry-driven cooperation targeting technology adoption in light of the strict regulatory framework for the financial sector is needed. The EBF welcomes the EU observers support in its EBF Cloud Banking Forum, working on respective guidance for adoption of public and hybrid cloud computing in a multi-cloud environment.

Cross-border coordination within the EU, and globally is fundamental to promote the scale-up of technological innovation and to prevent the creation of an unlevel playing field and regulatory arbitrage.

Fragmentation is already limiting the potential of technological developments of banks, which also affects the overall competitiveness of the EU. To foster financial services at a European and global level, we encourage the Commission to support Member States in coordinating and harmonizing their laws and regulations related to the financial services industry. This will help to create efficiencies, economies of scale and promote innovation. We support a competitive and innovative Digital Single Market and are committed to ensure protection and security for customers not just for regulatory risks but also to increase customers trust in the financial sector. Hence, we also recommend further initiatives, such as collaboration schemes which facilitate the interaction between banks, FinTechs and other stakeholders, to foster innovation, and new opportunities.

Assess the need for adapting the existing prudential frameworks to the new financial ecosystem, also to ensure a level playing field

Financial services providers are increasingly relying on technology companies to support delivery mechanisms for financial services. Technology companies are also increasingly entering financial services directly. Such trends will have an impact on the customers, the supply chain, incumbent financial institutions and their regulators and supervisors. Big technology companies are able to quickly scale up services due to network effects and large user bases. Their entry may accordingly over time significantly change market structures. This may require a review of how the EU financial legislative framework regulates firms and activities, in particular if technology companies were to become direct providers of specific services (e.g. lending) or a broader range of financial services or activities. This may also require a review of how to supervise the overall risks stemming from financial services of such companies.

Financial regulation should harness the opportunities offered by digitalisation – e.g. in terms of innovative solutions that better serve customers - while protecting the public interest in terms of e.g. fair competition, financial stability, consumer protection and market integrity. The Commission accordingly invite stakeholders' views on the potential impact of technology companies entering financial services and possible required policy response in view of the above public policy objectives.

Question 8. In which financial services do you expect technology companies which have their main business outside the financial sector (individually or collectively) to gain significant market share in the EU in the five upcoming years?

Please rate each proposal from 1 to 5:

	1 (very low market share - below 1%)	2 (low market share	3 (neutral)	4 (significant market share)	5 (very significant market share - above 25%)	N.A.
Intra-European retail payments	○	○	○	○	◉	○
Intra-European wholesale payments	○	○	○	◉	○	○
Consumer credit provision to households with risk taking	○	○	○	◉	○	○
Consumer credit distribution to households with partner institution(s)	○	○	○	◉	○	○
Mortgage credit provision to households with risk taking	○	○	◉	○	○	○
Mortgage credit distribution to households with partner institution(s)	○	○	◉	○	○	○
Credit provision to SMEs with risk taking	○	○	○	◉	○	○
Credit distribution to SMEs with partner institution(s)	○	○	○	◉	○	○
Credit provision to large corporates with risk taking						

	◉	○	○	○	○	○
Syndicated lending services with risk taking	○	◉	○	○	○	○
Risk-taking activities in Life insurance products	○	◉	○	○	○	○
Risk-taking activities in Non-life insurance products	○	◉	○	○	○	○
Risk-taking activities in pension products	○	○	◉	○	○	○
Intermediation / Distribution of life insurance products	○	○	○	◉	○	○
Intermediation / Distribution of non-life insurance products	○	○	○	◉	○	○
Intermediation / Distribution of pension products	○	○	◉	○	○	○
Other insurance related activities, e.g. claims management	○	○	◉	○	○	○
Re-insurance services	○	◉	○	○	○	○
Investment products distribution	○	○	○	◉	○	○
Asset management	○	○	◉	○	○	○
Others	○	○	○	◉	○	○

Please specify in which other financial services you expect technology companies to gain significant market share in the EU in the five upcoming years:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Financial Services is witnessing an unprecedented time of change with digital transformation redefining the entire industry and the recent interest of BigTech firms in the sector, represents a key factor. Among the several areas impacted, payments will be at the top of the list. New opportunities to make payments, in addition to cards and credit transfer and direct debit, have emerged in recent years and will likely be a driver for tech entrants to gain market share in the EU. In addition, technology companies are also expected to gain significant market share in the EU in the upcoming five years in the field of money transfer/remittances.

Technology companies could also potentially play a key role and gain a significant market share in areas of support to SMEs with ecommerce activities. Clear examples might be lending services offered to SMEs linked to their daily e-commerce volumes. Significant market share gains could also come from providing for the distribution channel of payments, insurance products and supply chain finance.
Other areas where technology companies could gain significant market share include:

- Digital Identity / KYC / Authentication and consumer financial advisory apps with more financial management automation.
- Capital markets and trading (e.g. new business areas such as trading and investments in cryptocurrencies and specialized trading for NPL).

Question 8.1 Please explain your answer to question 8 and, if necessary, describe how you expect technology companies to enter and advance in the various financial services markets in the EU Member States:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Business models for banks are changing also due to the role of BigTech firms. Just like the other technology companies, BigTech firms typically have a highly automated operation and an agile software development process, giving them the ability to quickly adapt their systems and services to users' needs. Moreover, they have typically established global operations and a large customer base. They can use a vast amount of information about their customers to provide them with tailored financial services. As often reported by different studies (Financial Stability Broad report on FinTech in Finance (2019); BIS Report Big tech in finance: opportunities and risks (2019); BIS Working Paper BigTech and the changing structure of financial intermediation (2019); Miguel de la Mano and Jorge Padill, BigTech Banking (2018)) these companies can rapidly gain a significant market share when launching a new financial product or service. In doing so, these companies can both collaborate/ add services on top of the existing financial structure (e.g. acting as a marketplace or distribution platform or leveraging existing card and inter-bank payment schemes to offer mobile wallets, payment initiation services or online acquiring services) or compete/offer services outside of the existing infrastructure. This makes it difficult to assess exactly the market share they might obtain in existing business models. This suggests the possibility of a deep transformation of the financial sector in which the structure and configuration of the market might be altered.

Regarding specific activities, BigTechs have so far focused on those areas that are subject to a less stringent regulatory framework, are not capital intensive or show higher ROEs, and are more complementary to their existing core businesses (e-commerce, social networks, etc.). This refers most notably to payments and credit-related services not involving deposit-taking, and in some cases, insurance. We expect this trend to continue going forward, although different BigTechs can be expected to devote more attention to specific areas depending on what reinforces the core of their digital ecosystems. Moreover, we expect these companies to obtain a more significant market share in those businesses in which they can leverage their competitive advantages - large customer bases and the ability to obtain relevant information on their customers.

As such, we would expect them to gain a significant market share in retail payments and in the provision of consumer credit, and medium to significant presence in other lending segments (e.g. to SMEs) or in the distribution of insurance products. Lending is a key priority in terms of revenues and number of companies and risk rating areas are now developing. SMEs represent the main target and one Big Tech firm is now able to offer loans to third-party sellers on the e-commerce platform. Looking at larger business clients, the trade services' market share might also be at risk.

For the moment, we do not expect them to gain a signinificant market share in those businesses that are very capital intensive or highly regulated (e.g. mortgage lending, risk-taking in insurance products) or where they benefit less from their competitive advantages (e.g. lending to large corporates). Moreover, even if in certain activities (e.g. asset management) these companies are not likely to become dominant providers of stand-alone services, they could become relevant actors if the activity is necessary to provide other services like store-or-value or payments (including in the form of stablecoins).

With this challenging context, once more we believe that it is crucial to ensure a full implementation of the principle of "same services, same risks, same rules and same supervision".

Question 9. Do you see specific financial services areas where the principle of "same activity creating the same risks should be regulated in the same way" is not respected?

- (●) Yes
- ( ) No
- ( ) Don't know / no opinion / not relevant

Question 9.1 Please explain your answer to question 9 and provide examples if needed:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

• The consolidated application of prudential requirements implies that banks' subsidiaries conducting the same activities as BigTechs (e.g. consumer lending, e-money, payment institutions) face an additional layer of requirements on top of those that are relevant for the activity in question. Therefore, when launching innovative solutions, companies who are part of EU banking groups face several competitive disadvantages vis-à-vis non-EU banks and non-bank entities. This is also particularly harmful in terms of reducing the flexibility that a bank can apply to its digital activities, even when they are not creating relevant risks to the

entity (either because the volume is reduced or because it is well separated) and make it challenging for banks to be able to innovate at the same speed (increasing the time to market) as those players who can apply more flexibility. Amongst the rules and policies that banks must always follow but that are not necessarily applied, or required, to other players include: prudential rules, governance requirements, compliance and conduct (financial crime, regulatory compliance (e.g. MIFID)), cybersecurity and T&O (Cyber and Risk technology); data Management, Technology and Operations (including CIO, architecture), accounting and financial information (incl. reporting requirements and consolidation of financial statements), internal audit, outsourcing and third party Management (third-party certification and risk assessment, management of outsourcing and third-parties, and Cloud Transfer), Human resources (suitability, identification of material risk takers and compensation principle), risk management (risk framework, appetite, models, systems, and controls).

- Non- banks do not have the constraints of software deductions. This creates an unlevel playing field for banks, affecting both organic innovation and the acquisition of FinTechs. When a bank invests in software, it needs to put aside similar level of capital to cover the CET1 requirements, in addition to the expense the bank actually made in the software. The moment a bank acquires a FinTech, this becomes particularly visible, since the bank needs to fully deduct all the value of the acquired software.
- The general potential to operationally implement new technology solutions in financial institutions depends very much on the regulatory framework and the strict financial regulation allowing for approval and flexible changes to service solutions. While banks are committed to their responsibilities under such framework, it does introduce procedures that other actors are not facing when considering to offer corresponding services. For example the wide definition of cloud solutions as outsourcing bears the risk of creating disproportionate requirements for even minor (far from being critical) IT solutions, as long as they have cloud hosting functions, e.g. An app with bank employee information carries a different risk than cloud-based lending solutions.

- Requirements regarding supervisor approval and expectations. E.g. on loan origination, non-bank players do not have the same limits regarding the documentation to be considered, the procedures, reporting. The lack of clarity on the supervisors' expectations regarding the use of AI for risk management and capital requirement calculations is another example.
- The fight against money laundering and terrorist financing (ML/TF). Advancing technology provides opportunities and incentives not only to market participants but also to criminals. In turn, ML/TF measures need to evolve, offering better detection and options to investigate. A regulatory framework that is fit-for-purpose is an important enabler to provide these tools. As an example, crypto-assets introduce technological features to be addressed e.g. when linking fiat and crypto currencies. Covering only one moment of the exchange would make it impossible to detect many illicit transfers. The same considerations could be applied to payment gateway providers. Accountability by new actors is important. Non-bank technology platforms operating in the financial sector on the basis of crypto-assets are also not sufficiently covered by AML regulation. The actual requirements for technology platforms should be the same as financial institutions, to the extent they provide the same services.
- Digital Wallet Providers, where transactions can be funded from an alternative deposit source / or card details tokenised for the purpose of e-commerce or mobile payments. Whilst consumers may deem this to the same activity, there are varying degrees of licencing structures with some wallet provides being outside of the scope the regulatory perimeter (given the underlying payment may be provided by the customer's bank).

Question 10. Which prudential and conduct risks do you expect to change with technology companies gaining significant market share in financial services in the EU in the five upcoming years?

Please rate each proposal from 1 to 5:

	1 (significant reduction in risks)	2 (reduction in risks)	3 (neutral)	4 (increase in risks)	5 (significant increase in risks	N. A.
Liquidity risk in interbank market (e.g. increased volatility)	○	○	○	○	◉	○
Liquidity risk for particular credit institutions	○	○	○	◉	○	○
Liquidity risk for asset management companies	○	○	◉	○	○	○
Credit risk: household lending	○	○	○	○	◉	○
Credit risk: SME lending	○	○	○	◉	○	○
Credit risk: corporate lending	○	○	◉	○	○	○
Pro-cyclical credit provision	○	○	○	◉	○	○
Concentration risk for funds collected and invested (e.g. lack of diversification)	○	○	○	◉	○	○
Concentration risk for holders of funds (e.g. large deposits or investments held in a bank or fund)	○	○	◉	○	○	○
Undertaken insurance risk in life insurance	○	○	○	○	○	◉

Undertaken insurance risk in non-life insurance	○	○	○	○	○	◉
Operational risks for technology companies and platforms	○	○	○	◉	○	○
Operational risk for incumbent financial service providers	○	○	○	◉	○	○
Systemic risks (e.g. technology companies and platforms become too big, too interconnected to fail)	○	○	○	○	◉	○
Money-laundering and terrorism financing risk	○	○	○	○	◉	○
Other	○	○	○	○	◉	○

Please specify which other prudential and conduct risk(s) you expect to change with technology companies gaining significant market share in financial services in the EU in the five upcoming years:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

- Financial stability risks, related to lending:
  - Moral hazard may increase relative to the status quo as platforms follow an originate-to-distribute model with small or very limited stakes in the loans generated.
  - Adverse selection is also likely to increase since platforms may have an incentive to price risk very low while searching for monetization in other markets. This could lead to a contagion effect in other players which may need to reduce their lending margins to protect their businesses.
- Financial stability risks related to bank disintermediation. Disintermediation of banks (from payment and other digital businesses), could result in compromising bank's ability to deliver other vital services (i.e. lending). The economy is dependent on banks' ability to lend and provide liquidity. Lending margins are low, and it is not clear they can shrink further without compromising the banks' ability to lend. If banks cannot power their lending with the digital business (and related customer relationship, relevance and knowledge gathering), the volume of lending might diminish. While a growing and deepening capital market may be able to compensate for falling bank lending, this will not compensate the risk of falling banks' capacity to do so. The entry of new lending providers, such as crowdfunding platforms, or the promotion of the capital market tools, is far from reaching the capacity to substitute banks. Even BigTechs, with more capacity to provide credit, may not have an interest in maintaining the commitment over the cycle, as banks and specialised players do. For BigTech, lending is a different business line that could be abandoned or promoted according to the economic conditions, profitability rates or any other strategic reason. However, for banks, lending is the core activity.
- Partial disintermediation of the value chain. In general it could be stated that a more unbundled banking sector with more complex value chains will lead to 'vertical' risks (e.g. outsourcing risk) than an integrated value chain, but also a shift in risk allocation in different parts of the value chain, which are potentially less visible and/or less regulated.
- The lifecycle of a financial service should be considered. Often the implications of misselling of a financial service may not be known for a number of years. Therefore, to the extent that technology firms gain market share in the financial service sector and offer services on a finite basis, or products become obsolete, this should be taken into account by regulators.
- The concentration power of Big Tech companies can allow them to leverage their data knowledge advantage and network effects to increase entry barriers in the Financial Services industry.

Question 10.1 Please explain your answer to question 10 and, if necessary, please describe how the risks would emerge, decrease or increase with the higher activity of technology companies in financial services and which market participants would face these increased risks:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

- Liquidity and funding risks could appear for the banking sector if BigTechs' activities in payments become of a significant volume. A relatively large pool of funds may be controlled outside of the banking

system. Although existing regulations require e-money/payment institutions to deposit these funds with commercial banks or in other highly safe and liquid assets as a means to ensure the safeguarding of customers' funds, this implies a change in banks' funding structures i.e. a significant proportion of retail funding would be replaced by wholesale funding, which may reduce the stability of bank funding and would increase banks' funding costs. This could eventually undermine the financial sector's role in financing long term investments. Even where BigTech firms provide an interface between providers of financial services and their customers (i.e. marketplace for deposits or payment initiation services), rather than competing directly with them, there remains some risks. Especially when coupled with instant payments, a widespread use of BigTechs' solutions in this field would facilitate rapid and large-scale movements of clients' funds, reducing the stickiness of bank deposits. This again could have implications on banks' cost and stability of funding as already described.

- Credit risk in the case of household lending, SME lending and corporate lending. How the risk is managed may be relevant, even if funds are not raised from the public, from the perspective of dependency.
- A rapid expansion of credit provision by BigTech firms could lead to enhanced procyclicality in credit provision, as funding flows from BigTechs could become large or unstable or concentrated in some market segments. The ability of BigTechs to maintain the credit supply during a downturn is also not clear. This might be due to a reduction in lending standards, a less stringent governance framework or the misalignment of incentives under an agency lending model. Also, there exists uncertainty on the performance of new forms of credit assessment which have not been tested through a full business and financial cycle. These risks are likely to become more prominent in those segments in which these companies can be expected to obtain a more significant market share e.g. consumer lending, SMEs lending.
- Operational risk for incumbent financial service providers: concentration of risk from many banks in a single point.
- Systemic risks (e.g. technology companies and platforms become too big, too interconnected to fail). Where BigTechs add new layers on top of existing services (for instance, as providers of a deposit or credit marketplace or as part of the payments infrastructure), they could become critical infrastructures for the functioning of the market. To the extent that they directly offer services to end-users, they could become themselves systemic providers of essential financial services for the economy such as lending, storing customers' savings or channelling payments. In both cases, their failure could cause widespread disruption to other parts of the financial system or the economy more broadly. Unlike existing regulations for banks, financial markets infrastructures and other providers of systemic importance, existing activity-specific rules seem unlikely to ensure the continuity in the provision of those essential services should an idiosyncratic or system-wide event take place. The interconnection with the economy may be bigger than banks. Given the key features of digital ecosystems and the competitive advantages, the systemic importance of BigTechs' services may not only materialize in a relatively short period of time, but it can reasonably be expected to increase over time.
- The phenomena of crypto-assets increases the potential of money-laundering and terrorism financing risk, should the established AML regulation allow for looopholes or grey zones for new market entrants applying this technology e.g. private stablecoin initiatives. Crypto-asset services should be added to the AML /CFT legal framework obligations. Policymakers should ensure that, together with legislative action and regulatory work on this field, FIUs, the ESAs and NCAs play a leading role promoting the knowledge, expertise, training and information sharing with banks, as well as the use of new IT solutions that might assist banks and other obliged entities in effectively understanding and handling the ML/TF risk factors raised by crypto assets/ crypto asset service providers. Effective capacity of public institutions and all the relevant AML/CTF stakeholders (not only banks) is needed to progressively identify, understand, and deal with the idiosyncrasies of virtual assets and with the specific structural elements of VASPs channels in a proactive way. A European or global identity standard could improve AML compliance in the crypto space by providing customers' KYC information that could help fulfilling mandatory AML requirements.

Question 11. Which consumer risks do you expect to change when technology companies gain significant market share in financial services in the EU in the five upcoming years?

Please rate each proposal from 1 to 5:

	1 (significant reduction in risks)	2 (reduction in risks)	3 (neutral)	4 (increase in risks)	5 (significant increase in risks	N. A.
Default risk for funds held in non-banks and not protected by Deposit Guarantee Scheme	○	○	○	○	◉	○
Liquidity risk	○	○	○	◉	○	○
Misselling of insurance products	○	○	○	◉	○	○
Misselling of investment products	○	○	○	◉	○	○
Misselling of credit products	○	○	○	◉	○	○
Misselling of pension products	○	○	○	◉	○	○
Inadequate provision of information	○	○	○	◉	○	○
Inadequate complaint and redress process and management	○	○	○	◉	○	○
Use/abuse of personal data for financial commercial purposes	○	○	○	◉	○	○
Discrimination e.g. based on profiles	○	○	○	◉	○	○

Operational risk e.g. interrupted service, loss of data	○	○	○	◉	○	○
Other	○	○	○	◉	○	○

Please specify which other consumer risk(s) you expect to change when technology companies gain significant market share in financial services in the EU in the five upcoming years:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The main issue arising from the increase market share of technology companies is that they do not comply with the same rules as the banking sector, despite offering the same services, thereby creating a risk that consumer protection is undermined. Other potential risks include:

- Consumer risks could arise in relation to some business models often employed by BigTech companies - marketplaces in which consumers can directly sign up to products from different providers. In this regard, consumers might struggle to differentiate who is the responsible party in such transactions (as well as its regulatory status and the responsible authority) and they might face inadequate complaint and redress processes. Moreover, in this context, the lack of a regulatory framework generates uncertainty as regards the allocation of liabilities, and whether the responsibility lies with the provider or with the platform. This might ultimately lead to an overburdening of the liability on the providers, which are regulated figures.
- A common theme from BigTechs operating in the digital wallet space is through the white labelling of digital financial products with partnerships with regulated entities. Given the customer relationship is generally held with the Big-tech, there may be a lesser level of operational and IT stability obligations /scrutiny (given they often do not require regulatory authorisation). Furthermore, the payment/transaction data will often be held by the technical provider for use of a wider set of use cases (such as sharing with third parties or for target promotions etc.). This may not always be made clear to customers.
- Information and transparency, in areas such as communication to customers, fair pricing, data breaches and protection, risk of fraud, financial exclusion of certain consumer segments, etc.
- Looking at the potential for concentration with BigTech providers, the EU competition law needs to be fit-for-purpose, continuing protection of consumers against detrimental effects of anti-competitive behaviour in the digital service market.
- With reference to crypto-assets and Initial Coin Offerings (ICOs), a potential risk for the customer is the lack of appropriate transparency in some cases. Disclosure requirements for new services and assets, proportional to the risk and use of the asset, are an important feature to deliver consumer and investor protection. A level playing field must be established with the existing regulatory framework and incumbents, applying the principle of “same services, same risks, same rules”. ICOs have been become known for their vulnerability to fraud in the last years. Transparency is one of the prerequisites when looking at the potential of this instrument. Even more so, to continuously uphold the existing level of consumer protection in financial services, the “misleading disclosure of information to consumers” (connected to -but different from- “inadequate provision of information” and misselling of investment products”) should be carefully considered when mapping future risks.

Question 11.1 If necessary, please describe how the risks would emerge, decrease or increase with the higher activity of technology companies in financial services and which market participants would face these increased risks:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The higher activity of technology companies in financial services and products would probably increase risks in relation to those areas that are not yet regulated in the same way for all the market participants carrying out the same activities. For instance, the EU framework for prudential supervision aimed at ensuring the stability of the financial market, is not applicable to non-banks, such as technology companies performing similar financial services activities. Market participants offering the same service or product should be regulated by rules that are activity-based and according to the risks that the specific activities produce. This principle should apply to all types of rules and regardless of whether the activities are carried out by a financial institution, or a BigTech.

Other risks include:

- Prudential risks and financial stability risks, particularly where concentration of customer/activity with unregulated entities, not subject to the same level of stress testing or prudential requirements.
- Increase in liquidity risk, reflecting the probability that non-financial entities will not be able to meet their financial commitments because the entity does not have the ability to liquidate assets sufficient to pay its obligations.
- Increase in the importance of analysis and appropriate approval of suppliers. In different situations, customers may not be aware of which kind of supplier they are dealing with, although this has clear implications in terms of protection. A clear example is the protection of deposits, which is not the same for e-money institutions or banks.
- Liability issues: Especially where the service is provided by the underlying bank (e.g. PISP model, where the customer's underlying bank will be liable to the customer in the first instance rather than the PISP, with the bank to recover funds from the PISP if liable). This may place an increased burden on the banks (despite not holding the service relationship) and may not be clear to customers.

Having said that, it is important to note that the likelihood of these risks materializing depends on the model of engagement chosen by BigTech companies. Indeed, in those models in which these companies collaborate with traditional financial sector providers, they could benefit from banks' long standing expertise in regulatory compliance and risk management functions.

Question 12. Do you consider that any of the developments referred to in the questions 8 to 11 require adjusting the regulatory approach in the EU (for example by moving to more activity-based regulation, extending the regulatory perimeter to certain entities, adjusting certain parts of the EU single rulebook)?

- (●) Yes
- ( ) No
- ( ) Don't know / no opinion / not relevant

Question 12.1 Please explain your answer to question 12, elaborating on specific areas and providing specific examples:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We believe that it is necessary to adapt the regulatory approach in the EU to ensure a level playing field in a context that is currently lacking between traditional financial institutions and other market participants. Current bank regulatory and supervisory frameworks generally predate the technologies and new business models of technology companies. This creates a risk of unintended regulatory gaps when new business models move critical banking activities outside regulated environments or, conversely, result in unintended barriers to entry for new business models.

EU authorities should promote innovation by all players under fair and even conditions by:

- Shifting from entity to activity-based regulation and supervision and moving to principle based rules.
- We encourage the Commission to raise the issue of the regulatory perimeter with regard to large technology companies at the G20 level, to ensure that the same activity is subject to the same regulatory obligations and the same conditions of supervision irrespective of whether the provider is a bank or a non-bank company. The EBF would be happy to support the Commission in this endeavour.
- Non-bank subsidiaries of banking groups should be subject to proportional prudential requirements, or eventually, be taken out of the regulatory perimeter, provided adequate isolation of risks , so that non-core banking activities of banking groups are not constrained by the burden of prudential regulation and supervision that was not conceived for such activities. This would enable banks to compete on an equal footing with non-bank providers.
- Authorities should consider whether some of the business models not previously covered by regulation should be brought into the regulatory perimeter and be subject to targeted obligations regarding AML/CFT, reporting or consumer protection as deemed adequate.
- Some of the activity-specific licensing and supervisory frameworks in place might need to be revisited to ensure their fitness for the potential risks of large-scale provision of these services by the BigTechs.
- Authorities should find a way to address BigTechs' systemic dimension, either by enhancing the monitoring of non-bank providers of finance or amending macroprudential policies and tools to ensure they are fit to deal with the accumulation of risks outside of the banking sector. Authorities could also consider defining a set of criteria and requirements for systemic non-bank providers of key financial services. Risk of banks disintermediation should also be assessed to ensure it this does not affect financial stability.
- Embedding Open Banking into the broader context of the Data Economy and levelling the playing field as regards access to data. PSD2 has stimulated competition and innovation, however it has also created an asymmetry in terms of access to data: with the consent of the customer non-financial firms can access financial transactions, but their users cannot easily share the data held in those firms. The EU needs a cross-sectoral framework to empower both individuals and firms, ensuring that they can share their data when and with whom they want. We support enhancing the existing right to data portability under Article 20 GDPR, as proposed by the Commission in its Data Strategy, and introducing data portability for individuals under the proposed ex-ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers. We also encourage the Commission to explore a portability right for firms, starting with the ability of businesses to port their data from large digital platforms through the ex-ante regulatory instrument.
- Adapt competition policy and regulation to the challenges of digital markets. Focus on dynamic competition and risks to innovation, taking data (and the role of data gatekeepers) fully into account. Merger control thresholds that capture firms with low turnover but highly competitive potential. Introduce ex ante regulation when needed, e.g. neutrality requirements for key digital platforms to ensure fair access to platforms and infrastructure that are relevant for the delivery of financial services,
- In order to ensure a consistent protection against money laundering, there cannot be an unjustified differentiation between traditional financial institutions and other market participants. Ensuring that crypto assets service providers comply with the same rules as financial institutions would make it easier for the latter to engage in doing business with such providers, if able to deliver KYC information.
- While crypto-assets need to be assessed in a balanced way, considering both innovative potential and challenges, the principle "same services, same risks, same rules" should be the foundation of such assessment and following regulatory approach.

Enhance multi-disciplinary cooperation between authorities

The regulation and supervision of Digital Finance requires more coordination between authorities in charge of regulating and supervising finance, personal data, consumer protection, anti-money-laundering and competition-related issues.

Question 13. Building on your experience, what are the main challenges authorities are facing while supervising innovative/digital players in finance and how should they be addressed?

Please explain your reasoning and provide examples for each sector you are referring to (e.g. banking, insurance, pension, capital markets):

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Challenges include:

- The pace of evolution of new technologies makes it difficult for authorities to keep up to speed with the latest developments, which can result in reactive decisions and partially contradictory/conflicting objectives. In addition, regulation and the institutional architecture are often siloed.
- Lack of necessary skills and technical expertise among financial authorities to regulate and supervise new business models and uses of technology in finance. This often leads to conservative stances that leave banks in a situation of an unlevelled playing field versus new digital players.
- The scope of financial services is blurring– who is the regulatory/ supervising authority? For new innovative products and services emerging in the market, it is not always clear if and which regulatory frameworks are applicable and supervisory authorities only have the mandate to supervise regulated entities. Problems in this regard are the fragmentation of the national regulatory regimes within EU and discrepancies between the banking regulatory law, other legislation, and legal precedents. Examples include:
  - In regards to outsourcing, even if there are some base principles established by the applicable regulation and certain interpretation requirements set out by the EBA in their guidelines on outsourcing, there is an asymmetry among the requirements demanded by the NCA depending, on which entity is outsourcing a function, and the provider. The regulatory requirements on outsourcing matters should be demanded equally both for the outsourcing entity and for the service provider.
  - In respect of payments, it can be unclear whether all European regulators apply the same standards when providing the authorisation to become a payments provider. Once a licence has been granted, that provider can then passport into other jurisdictions which may therefore mean there are different levels of scrutiny applied to providers in the market.
  - Onboarding procedures, where diverging views in each country are creating a patchwork of solutions in the market, which respond to regulatory requirements rather than robustness, efficiency, or customer service needs.
- Challenges in ambiguity of interpretation.
- Activities of different market participants around digital finance are often cross-border by nature, which may lead to challenges if the supervisory approaches in different member states are not coordinated.
- It is a challenge for regulators and supervisors is to pair an innovative mindset with a continuing focus on mitigating risks

Finally, many of the challenges created by these new players in finance (e.g. related to competition, data

protection or privacy, the creation of new critical infrastructures for the global economy, tax etc.) expand beyond the financial sector, and thus of the remit of financial authorities. Without coordination, this may cause inconsistencies in their approaches. Digital markets and new digital players are inherently global, and thus are difficult to govern within national borders. As a result, national authorities often lack adequate mechanisms to apply domestic policies to global companies.

The challenges can be addressed by:

- Regulatory sandboxes are a useful tool for authorities to better understand innovation while testing new, innovative solutions in a safe environment, and to identify regulatory barriers to innovation that may exist. Having all relevant authorities- either financial or non-financial (Data Protection authorities, Competition authorities, AML authorities, etc.) - participating at the same time in sandbox projects would also help to enrich and provide more value to this environment, helping to ensure that when something is approved/allowed or decided within a sandbox environment, it holds up towards all regulators.
- A framework for cooperation among different national sandboxes regimes, from different countries, will also help to create synergies among the different authorities, while also contributing to harmonization. We therefore continue to support the work of EFIF as it would help to better understand and face barriers for cross-border innovation in the European financial sector.
- In respect of payment, agreed standards for authorising new entities could be implemented on an EU wide basis.
- Including innovation as part of the mandate of supervisors.

Question 14. According to you, which initiatives could be put in place at EU level to enhance this multi-disciplinary cooperation between authorities?

Please explain your reasoning and provide examples if needed:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

To enhance multi-disciplinary coordination between authorities, we recommend:

- To continue supporting the European Forum for Innovation Facilitators (EFIF) to provide for cross-border testing. This will help regulators and supervisors to better understand technology applications and relevant risks, as well as to accelerate learning through sharing of knowledge and best practices.
- Enhancement of the use of RegTech, originally aimed at improving compliance processes at financial institutions level, which if effectively developed, could create opportunities to not only automate regulatory reporting and compliance requirements but also facilitate more cross-sectorial and cross-jurisdictional cooperation for improved compliance (e.g. AML/CFT). See the relevant section in the consultation for further recommendations on RegTech.
- To continue promoting public-private dialogue with all relevant stakeholders.
- Adopting authorization procedures in a coordinated manner, including making joint decisions especially for cross border projects, so that the implementation is smoothed.
- Establishing a framework grid and taskforce to link all authorities to discuss overlaps and ensure an aligned approach. Through a broad regulatory view, authorities can align views to ensure coordinated application across authorities.

Finally, coordination among authorities is critical, this should not only include financial authorities, but also those responsible for data protection, cybersecurity, etc. Cross-country and cross-sectorial coordination and exchange of information with regard to innovation and the use of new technologies should be ensured.

II. Removing fragmentation in the single market for digital financial services

Removing Single Market fragmentation has always been on the radar of EU institutions. In the digital age, however, the ability of firms to scale up is a matter of economic productivity and competitiveness. The economics of data and digital networks determines that firms with substantial network effects enjoy a competitive advantage over rivals. Only a strong Single Market for financial services could bring about EU-wide businesses that would be able to compete with comparably sized peers from other jurisdictions, such as the US and China.

Removing fragmentation of the Single Market in digital financial services while maintaining an adequate level of security for the financial system is also essential for expanding access to financial services for consumers, investors and businesses across the EU. Innovative business models and services are flourishing in the EU, with the potential to bring greater choice and better services to consumers. Traditional players and start-ups are both competing, but also increasingly establishing partnerships to innovate. Notwithstanding the opportunities provided by the Digital Single Market, firms still face obstacles when scaling up across the Single Market.

Examples include a lack of consistency in the transposition, interpretation and application of EU financial legislation, divergent regulatory and supervisory attitudes towards digital innovation, national 'gold-plating' of EU rules, cumbersome licensing processes, insufficient funding, but also local preferences and dampen cross-border and international ambition and entrepreneurial spirit and risk taking on the part of business leaders and investors. Likewise, consumers face barriers in tapping innovative digital products and being offered and receiving services from other Member States other than of their residence and also in accessing affordable market data to inform their investment choices. These issues must be further addressed if the EU is to continue to be an incubator for innovative companies that can compete at a global scale.

Question 15. According to you, and in addition to the issues addressed in questions 16 to 25 below, do you see other obstacles to a Single Market for digital financial services and how should they be addressed?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

To compete successfully in the new environment, financial service providers need to obtain efficiency and scale. They should be able to leverage technological developments for cross-border provision of financial services, at least within the EU Single Market. The lack of a well-functioning Single Market and effective harmonisation in the rules, supervision and enforcement does not only impair the cross-border provision of services, but could give rise to risks for financial stability, integrity, and the protection of consumers. This fragmentation might be due to:

- The lack of an EU framework for certain services (e.g. crypto-related activities); for conduct rules (e.g. as noted by the ESAs in a 2019 report, there are no unified general conduct rules, and there is insufficient harmonization between different activity-specific level 1 rules).
- No definition of what constitutes cross-border business, creating difficulties to identify which authority is responsible for the supervision.
- Insufficient harmonization in the implementation and enforcement of the EU framework, for example:
  - The uneven transposition of Directives:

AML minimum harmonisation directive leading to differences in national implementation. Regulation for remote onboarding in different member states and also to client's identification verification requirements.

PSD2 transposition in Spain leading to different AML requirements for banks versus non-banks providing account information services.

IBAN discrimination, local unique payment methods.

The implementation of the mechanical procedure for e-signature differs among member states.

- Lack of supervisory convergence. Supervisory authorities in different countries often follow divergent practices as regards authorisation and licensing. On the one hand, businesses willing to operate in several jurisdictions often find language barriers and different or rigid formats and communications methods.
- Financial service providers often find difficulties in exercising passporting rights, especially without a physical establishment. In most EU member states, authorities require compliance with local prudential or AML/CFT rules, although as a passported entity the applicable framework is the one from the home member state. As a result, the cost of having to comply with local rules (e.g. need to hire local law firms or ad-hoc compliance studies when rules are not adequately harmonized), in addition to the aforementioned language barriers, can make the scale up to other jurisdictions unaffordable or unattractive for the providers, thereby directly conflicting with the Digital Single Market.
- At the moment, there is no public register covering all member states, from which one could, for free, obtain information regarding companies' business identity codes, financial statements, or company representatives, for example. This can cause barriers to a Single Market and the free movement of services.

Finally, digital education is key to unlock the full potential of the digital single market and we strongly recommend improving initiatives to foster it.

Facilitate the use of digital financial identities throughout the EU

Both start-ups and incumbent financial institutions increasingly operate online, without any need for physical establishment in a particular jurisdiction. Technologies are enabling the development of new ways to verify information related to the identity and financial situation of customers and to allow for portability of such information as customers change providers or use services by different firms. However, remote on-boarding relies on different technological means (e.g. use of biometric data, facial recognition, live video) to identify and verify a customer, with different national approaches regarding their acceptability. Moreover, supervisory authorities have different expectations concerning the rules in the 5th Anti-Money Laundering Directive permitting reliance on third parties for elements of on-boarding. The Commission will also consult shortly in the context of the review of the EU Anti-Money Laundering framework.

Question 16. What should be done at EU level to facilitate interoperable cross-border solutions for digital on-boarding?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N.A.
Harmonise rules governing customer due diligence requirements in the Anti-Money Laundering legislation	○	○	○	○	◉	○

Harmonise rules governing the acceptable use of remote identification technologies and services in the Anti-Money Laundering legislation	○	○	○	○	◉	○
Broaden access for obliged entities to publicly held information (public databases and registers) to enable verification of customer identities	○	○	○	○	◉	○
Provide further guidance or standards in support of the customer due diligence process (e.g. detailed ID elements, eligible trusted sources; risk assessment of remote identification technologies)	○	○	○	○	◉	○
Facilitate the development of digital on-boarding processes, which build on the e-IDAS Regulation	○	○	○	○	◉	○
Facilitate cooperation between public authorities and private sector digital identity solution providers	○	○	○	○	◉	○
Integrate KYC attributes into e-IDAS in order to enable on-boarding through trusted digital identities	○	○	○	◉	○	○
Other	○	○	○	◉	○	○

Please specify what else should be done at EU level to facilitate interoperable cross-border solutions for digital on-boarding:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Implementation of know-your-customer (KYC) rules according to the 4th and 5th Anti-Money Laundering Directives (AMLDs) differs significantly across EU member states. An illustrative example consists of the differing requirements imposed on obliged entities when verifying the information on beneficial owners and

the intensity and time allowed to review, periodically, customer information and documents.

In this regard, an AML Regulation should be in place to set out clear and uniform rules for harmonising the KYC policy across the EU, making sure it is aligned with international standards and the FATF Guidance. In addition, such rules need to be followed up with clear guidance on how to implement specific provisions and include risk-based KYC requirements for specific topics. A document-based approach to KYC is rapidly becoming unsustainable in an increasingly digital world.

It would also be important to arrive at universally accepted definitions and terminology so that all relevant parties can share a mutual understanding on the key concepts. For example, AML laws make an important distinction between identifying a customer (or her/his representative, ultimate beneficial owner, family member, close business associate, etc.) and verifying her/his identity. As regards customer verification, AMLDs require that it should be done “on the basis of documents, data or information obtained from a reliable and independent source”. Instead of providing a detailed list of technical specifications, the only requirements are that the source of the information, etc. used must be reliable and independent. However, no criteria for the assessment of the source’s reliability, etc. are provided. The forthcoming AML legislative reform proposals should be more specific in terms of information to be collected and used (i.e. by illustrating different ways in which the KYC requirements based on the type of entity the obliged entities deal with). Basic customer data which are defined under clear and comprehensive rules should be collected in line with the RBA, including simplified due diligence flexibility on timing and means where appropriate or supplemented by additional risk-based measures.

Against this background, digital identity measures should not understate the risks arising from vulnerabilities in the unregulated sector (e.g. providers of digital ID systems) and inconsistencies in national and regional guidelines. Both issues make it more challenging for banks to assess the adequacy of digital ID systems. Basic customer data defined under clear and comprehensive rules should be collected in line with a risk-based approach, including simplified due diligence flexibility on timing and means, where appropriate, or supplemented by additional risk-based measures.

The EBF welcomes a flexible, risk-based approach that would support financial inclusion, as indicated by the FATF guidance on digital identity. As described in the guidance, AML/CFT risks may be mitigated by, for example, limiting the services available to the customer. However, this risk-based approach should have a broader scope beyond financial inclusion, enabling regulated entities to adjust customer due diligence (CDD) process to the risks of the specific services being offered at onboarding, and develop stronger confidence in the identity of their customers, as they require services of higher risks.

CDD is not a static exercise; this approach would help to reduce onboarding costs for regulated entities while improving customer experience and ultimately increasing conversion rates, while at the same time keeping AML/CFT risks under control. In addition, there would be merit in having guidance on the use of digital identity in the onboarding processes of legal persons, which also shares many of the potential benefits described in the FATF guidance on digital for their use by natural persons.

Currently, the European market for digital identity services is fragmented and unstructured. The digital identity ecosystem is distributed across multiple national approaches, regulatory environments, levels of digital governance, culture, and different levels of trust in institutions.
We would like to emphasize that we are currently facing an AML/CFT regulatory and supervisory fragmentation. In addition to a regulatory harmonisation, we therefore also need to harmonise the supervisory practice across EU member states, to ensure better coordination between national supervisors and to establish some kind of centralisation of supervisory powers at EU level.

Question 17. What should be done at EU level to facilitate reliance by financial institutions on digital identities gathered by third parties (including by other financial institutions) and data re-use/portability?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
Make the rules on third party reliance in the Anti-Money Laundering legislation more specific	○	○	○	○	◉	○
Provide further guidance relating to reliance on third parties for carrying out identification and verification through digital means, including on issues relating to liability	○	○	○	○	◉	○
Promote re-use of digital identities collected for customer due diligence purposes in accordance with data protection rules	○	○	○	○	◉	○
Promote a universally accepted public electronic identity	○	○	◉	○	○	○
Define the provision of digital identities as a new private sector trust service under the supervisory regime of the eIDAS Regulation	○	○	○	◉	○	○
Other	○	○	○	◉	○	○

Please specify what else should be done at EU level to facilitate reliance by financial institutions on digital identities gathered by third parties (including by other financial institutions) and data re-use/portability:

5000 character(s) maximum

Reliance on third parties is a growing and very relevant issue for financial institutions, especially following the outbreak of COVID-19. We welcome that the EU eIDAS Regulation provides for a conformity assessment body to ensure the compliance of qualified trust service providers and the services they provide against the requirements set out in the Regulation, which could also serve as a model for digital identity providers. In addition, the identification systems at the "substantial" level of assurance that are provided under the eIDAS Regulation are based on a two-out-of-three-factor authentication, including possession, knowledge, and inherence. Hence, the loss of one of the two factors is not sufficient to compromise the digital identity as compared to face-to- face procedure. A simple identity theft is therefore less likely, rather the second factor would have to be stolen in addition to the knowledge or possession element. The eIDAS Regulation also requires a high level of technical protection of data, keys, and factors, e.g. by encrypting and signing data. Thus, it is less likely to hack passwords or existing inherence factors from the database of the digital ID provider. Misuse of the digital identity is therefore mostly possible if the customer makes both factors available to a fraudster consciously or recklessly. With regards to security controls, 'identity' providers issuing the credentials will have to comply with specific security requirements provided by law, in order to ensure credentials' confidentiality and security. If the issuing phases are performed via processes that are not robust enough, they will affect/invalidate the identity itself used in the identification phase.
Based on a regulatory framework, regulated identity platforms in addition to regulated financial institutions could serve as reliable "third parties" and provide for better re-use and portability of data. In consequence, such regulated identity platforms can serve as a key-enabler for the EU digital economy. In this context, harmonization of regulations for the EU's financial sector is of utmost importance. However, we strongly encourage the Commission to take the issue of harmonized KYC and electronic ID requirements one step further and advocate for a cross-sectoral recognition of identification methods between different (regulated) industry sectors (such as finance, health, mobility, telecommunication) and the public sector in the EU. Cross-sectoral standardization with regard to KYC and quality of electronic identities could be achieved via the eIDAS Regulation and an enhanced used of qualified electronic signatures (QES). Yet, it must be noted that there are different ways to implement identity providers that financial institutions could rely on.
To the extent that firms were able to rely on digital identities gathered by other institutions, this would promote portability and improve efficiency from an onboarding perspective. However, we note that in respect of 'reliance', there a number of issues that need to be considered:
o A digital identity cannot be viewed as a 'singular' data point. An identity is made up of a number of data attributes and in order to ensure that 'reliance' can be placed on third party identities, firms must be in a position to trust the source of each data attribute. The focus should therefore be on creating a framework of data attributes that will enable firms to verify each of the attributes that are provided.
o AMLD4 introduced new requirements around the concept of 'reliance'. As such, it can become more onerous to rely on third parties for KYC processes than it is to undertake the KYC yourself.
Financial Institutions need laws that allocate the responsibility when they rely on third parties. Questions around liability in case of third-party reliance for KYC should be clarified in particular. This would therefore need to be considered as part of any guidelines or regulation that looks to facilitate the use of third-party digital identities from an AML perspective. That said, it is crucial to highlight the importance of having a comprehensive and internationally agreed digital identity assurance framework that can facilitate the use of harmonised digital identity systems across jurisdictions. This would also help to remove frictions when providing services across-borders, while ensuring the appropriate level of reliability for the digital ID solution used in light of the potential ML/TF, fraud, and other illicit financing risks. Best practices or lists of reliable digital identity systems or solutions would be appreciated, in order to create a global and trustworthy ecosystem on the basis of the FATF approach.
Creating and maintaining a digital identity ecosystem is very burdensome, as it involves technology, transparency, and security. Success comes from open source technology, interoperability across sectors and geographies, and public/private collboration.

Question 18. Should one consider going beyond customer identification and develop Digital Financial Identities to facilitate switching and easier access for customers to specific financial services?

Should such Digital Financial Identities be usable and recognised throughout the EU?

Which data, where appropriate and in accordance with data protection rules, should be part of such a Digital Financial Identity, in addition to the data already required in the context of the anti-money laundering measures (e.g. data for suitability test for investment services; data for creditworthiness assessment; other data)?

Please explain your reasoning and also provide examples for each case you would find relevant.

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Yes, going beyond customer identification and developing Digital Financial Identities to facilitate switching and easier access for customers to specific financial services could be explored. As digitalisation continues and is less bound by borders, Digital Financial Identities that are usable and recognized throughout the EU and go beyond pure customer identification, to also enable authorization of decisions could be very useful. It should, however, not become more difficult for consumers to make well-informed financial decisions. While we agree that digital channels for product switching should be enabled, Digital Financial Identities should not lead to reduced access to adequate advice.
A Digital Financial Identity could also be highly beneficial for fast and easy on-boarding, especially if usable and recognized throughout the EU and both in public and private sectors. Only a harmonized cross-sectoral approach will provide for the required market penetration with regard to digital identities. We therefore suggest a combined initiative of private and public stakeholders. In our opinion, at this point in time a Digital Financial Identity does not require any further data than is already required by the multitude of existing laws and regulations such as AML regulations, tax law and others. However, where suitable and based on a careful balancing with affected data protection principles, additional identification attributes and data could be obtained where legitimate. In this context, regulated identity platforms could provide users and regulated entities alike with both safe data storage and convenient (AML and GDPR-) compliant re-use of (verified) identification attributes and additional data.

Question 19. Would a further increased mandatory use of identifiers such as Legal Entity Identifier (LEI), Unique Transaction Identifier (UTI) and Unique Product Identifier (UPI) facilitate digital and/or automated processes in financial services?

- (●) Yes
- ( ) No
- ( ) Don't know / no opinion / not relevant

If yes, in which framework(s) is there the biggest potential for efficiency gains?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Although we support the mandatory use of identifiers such as Legal Entity Identifier (LEI), Unique Transaction Identifier (UTI) and Unique Product Identifier (UPI) and while we believe that they would help facilitating digital and/or automated processes in financial services and bring efficiencies, we would however like to point out that the mandatory use should be an obligation for the addressee of such a provision and not a direct or indirect obligation for the intermediaries carrying out services for such addressees. This means that the end-user, which is the entity to be identified, should have a LEI available and should be responsible for its use, its maintenance and updating. When obliging the intermediary instead of the end-user, many operational problems arise which can result in burdensome processes and severe financial damages. The EMIR or MiFID II provisions may serve as an example.

One of the main challenges for the industry has been and remains the barriers and difficulties for Non-Financial Counterparties or even entities that do not have legal personality to obtain, first, and then renew those identifiers, especially LEI. In some cases, they need the LEI even for situations that took place a long time before the reporting obligations started. In addition, different procedures and requirements across member states also can serve as a barrier.

Any framework demanding the use of identifiers should therefore clarify the legal consequences for the end-user who does not or cannot provide the required identifier (e.g. no LEI no trade). Regarding the use of UTIs, a globally harmonized approach and interpretation of its composition is essential. The same goes for the question which party is to generate the UTI.

As regards investment services, transparency, and data reporting, in general terms, the use of unique identifiers could represent a catalyst to further spread the adoption of digital and automated solutions across the entire financial services' industry. More in detail though, there are some challenges to be tackled in order to deliver such potential:

- Unique identifiers will have to fully comply to global standards, otherwise processing of large non-standardized data will reveal, in the long term, unsustainable (operationally and economically).
- A structured framework for the authentication of identifiers is also a crucial prerequisite, in order to achieve a thorough acceptance of data across markets.
- Centralization of data management will be essential, achieving a well-organized and steadily-structured collection of data, easy to store and access.

The actual use of such identifiers will have to be framed in clear unequivocal rules, so as to remove any

need for bilateral agreements among counterparties to a trade/contract, as such agreements would determine a time-absorbing and complex-to-manage network of relations, uneasy to leverage upon even in case of disagreements/litigations (as for instance it is demonstrated by the operational experience in the application of some parts of the EMIR Regulation).
With regard to payments, the identifiers that are already being used suffice both for Payment Service Providers (PSP) and Payment Service Users. For the latter, the use of Legal Entity Identifier is not widespread and would not be applicable for debtors and creditors that are not “legal entities”. However, for identifying Payment Service Providers and routing payments, the BIC code should remain the main identifier’ to address this.

Make it easier for firms to carry out technology pilots and scale up across the Single Market

Currently, three national competent authorities have established regulatory sandboxes with five more under development. Regulatory sandboxes are most often schemes to enable firms to test, pursuant to a specific testing plan agreed and monitored by a dedicated function of the competent authority, innovative financial products, financial services or business models. Besides, almost all competent authorities have established innovation hubs. Innovation hubs provide a dedicated point of contact for firms to ask questions to competent authorities on FinTech related issues and to seek non-binding guidance on regulatory and supervisory expectations, including licensing requirements. The European Forum of Innovation Facilitators (EFIF) is intended to promote greater coordination and cooperation between innovation facilitators established by financial sector supervisors to support the scaling up of digital finance across the Single Market, including by promoting knowledge-sharing between innovation hubs and facilitating cross-border testing in regulatory sandboxes.

Question 20. In your opinion (and where applicable, based on your experience), what is the main benefit of a supervisor implementing (a) an innovation hub or (b) a regulatory sandbox as defined above?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We support the idea of innovation hubs, as they can promote the exchange between supervisors and innovators. This can help firms to better understand which stance supervisors will take on interpreting the existing regulation, while supervisors can get a better overview over current market developments and insight into technological developments. However, to our understanding an innovation hub does not offer as close cooperation and exchange as a sandbox. Therefore, we would urge more countries to set up sandboxes that allow close cooperation between innovators and supervisors, a quick exchange on feasibility and on rules that apply.

In highly regulated industries such as financial services, compliance requirements and regulatory uncertainty hinder innovation, as they might delay and increase the costs of bringing innovation to the market. If adequately implemented, regulatory sandboxes offer promising benefits for all the parties involved, as they can promote the exchange between supervisors and innovators. In addition, availability of anonymised perspectives and learnings from regulators on activities within the sandbox would be useful.

More specifically, benefits of regulatory sandboxes include:
• For firms, they provide the opportunity to test products and services in a regulated environment and reduce time-to-market and costs. This allows financial entities the possibility to bolster their innovation projects and learn faster, while at the same time fine-tuning their value propositions. It also supports the

development of new, fully digital, and compliant cross-border services.

• From the supervisory point of view, a regulatory sandbox will help authorities to increase their knowledge on technology-based financial innovations, and to identify unnecessary barriers to innovation that may exist in the regulatory framework for the financial sector. It is key that these learnings are subsequently transferred to regulation/supervision with a view to removing these barriers. They also facilitate the understating of costs, risks, and opportunities of new solutions, and foster a better understanding of new business models and technologies.

• For policy makers, it allows them to understand how innovate use cases fit or do not fit in the current regulatory framework. If there is no understanding of a use case, it is impossible to regulate the use case (if necessary) appropriately. A regulatory sandbox can help with this challenge.

We therefore welcome the ongoing attention of supervisors and regulators to testing frameworks in Europe and would recommend to promote regulatory sandboxes at European level, as this can foster the Digital Single Market, which allows scaling and delivering innovations to all citizens across the EU, while also bolstering the EU's competitiveness with other leading markets as a hub for innovation and talent attraction. In this regard, the level playing field should also be respected in terms of different market players. It is important to make sure that these possibilities are not only open for the new market players but for all market players.

We would also recommend that, in the implementation of sandboxes, there is hands-on support from regulators as part of the project team, an ability to test new propositions with real customers and the ability to scale up from the sandbox. There should be collaboration with other relevant authorities, notably data protection supervisors.

Question 21. In your opinion, how could the relevant EU authorities enhance coordination among different schemes in the EU?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
Promote convergence among national authorities in setting up innovation hubs and sandboxes, through additional best practices or guidelines	○	○	○	○	◉	○
Facilitate the possibility for firms to test new products and activities for marketing in several Member States ("cross border testing")	○	○	○	◉	○	○
Raise awareness among industry stakeholders	○	○	○	◉	○	○

Ensure closer coordination with authorities beyond the financial sector (e.g. data and consumer protection authorities)	○	○	○	○	◉	○
Promote the establishment of innovation hubs or sandboxes with a specific focus (e.g. a specific technology like Blockchain or a specific purpose like sustainable finance)	○	○	○	◉	○	○
Other	○	○	○	○	◉	○

Please specify how else could the relevant EU authorities enhance coordination among different schemes in the EU:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

• Cross-border coordination within the EU is fundamental to promote the scale-up of technological innovation and to prevent an unlevel playing field or regulatory arbitrage. This is the principle underpinning the EU framework for experimentation.
• Coordination across EU member states should be enhanced. This would imply at least the possibility for a national authority to rely on the outcome of the testing done by another authority within a national sandbox via a system of mutual recognition.
• The European Forum for Innovation Facilitators (EFIF) should take the role as the central hub, facilitating exchange of information as well as the gathering of legal interpretations of existing regulations by national authorities in order to support the uptake of common approaches. We would welcome the establishment of dedicated guidance, building on the ESAs' best practices, seeking to harmonize the use of regulatory sandboxes across the EU, so as to ensure a level playing field across the Single Market and facilitate cross-border businesses to scale up.
• The Commission and the ESAs should monitor the outcomes of the testing conducted in national regulatory sandboxes and leverage the learnings obtained to improve the EU financial services regulatory framework. In particular, the Commission and the ESAs should ensure that regulation or standards that are proven to be unfit for the digital age as a result of the sandbox are adapted accordingly. The ESAs should build on the results of the EFIF and consider the establishment of an EU-level regulatory sandbox.
• To maximize the benefits of sandboxes, we also recommend that sandboxes have the broadest scope possible, and even to promote cross-sectoral sandboxes and ensure the involvement (when possible), or close cooperation of relevant authorities beyond the financial space, responsible for oversight of regulatory functions such as conduct authorities, data protection authorities, and financial intelligence units.
• Finally, the EFIF should link to relevant international initiatives, such as the Global Financial Innovation Network (GFIN,). Likewise, it is important to keep in mind similar initiatives that are promoted in third countries, as well as the GFIN work, to ensure knowledge sharing and to avoid a regulatory/innovation arbitrage.

Question 21.1 If necessary, please explain your reasoning and also provide examples for each case you would find relevant:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Question 22. In the EU, regulated financial services providers can scale up across the Single Market thanks to adequate licenses and passporting rights.

Do you see the need to extend the existing EU licenses passporting rights to further areas (e.g. lending) in order to support the uptake of digital finance in the EU?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In general, we support passporting rights and licenses, as they help to scale up innovations, foster the creation of a (digital) European single financial market and lead to products being offered to a broader audience in the EU. However, one precondition is that passporting rights are only created for areas where there are, or there should be, equivalent rules in every member state, in order to guarantee a level playing field and adequate consumer protection. Therefore, relevant areas should be carefully identified if existing rules are, or should be, equivalent and then a passporting right should be introduced, allowing institutions to scale up.

Currently there are some challenges in the supervision of the service providers acting based on passporting, due to a lack of clarity as regards the distribution of powers between home and host financial supervisory authorities. These challenges should be carefully considered before extending the passporting rights to any further areas.

Finally, in terms of certain areas, further harmonization of the on-boarding procedure in terms of client identification would be welcomed. This would avoid the necessity of the client to pass through the same identity verification procedure in the different countries.

Ensure fair and open access to relevant technical infrastructures for all financial service providers that wish to offer their services across the Single Market

(It should be noted that this topic is also included, from the payment perspective, in the Retail Payments consultation)

The emergence of providers of technical services supporting the provision of financial services bring both opportunities and challenges. On the one hand, such providers can facilitate the provision of cross-border services. On the other hand, they may in certain cases limit access to the platform or relevant devices' interface, or provide it under unfair and non-transparent terms and conditions. Certain Member States are starting to take measures in this respect.

Question 23. In your opinion, are EU level initiatives needed to avoid fragmentation in the Single Market caused by diverging national measures on ensuring non-discriminatory access to relevant technical infrastructures supporting financial services?

Please elaborate on the types of financial services and technical infrastructures where this would be relevant and on the type of potential EU initiatives you would consider relevant and helpful:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As a result of the ongoing digitalization of the economy and the changes in how customers engage with a wide variety of markets, access to digital or technical infrastructure outside of the traditional financial sector is increasingly important for the provision of financial services.

Key changes to customer behaviour include the rapid rise of e-commerce (and associated electronic payments); the use of digital wallets to make payments, often via mobile or other devices such as voice assistants; and direct access to existing or new financial services providers and products via internet enabled devices.

These activities are underpinned by a new set of technical infrastructure, including:

- Devices and their associated functionality, such as biometric authentication or communication protocols like Bluetooth and near field communication (NFC).
- App stores and pre-installed apps on devices.
- POS devices.

However, this infrastructure is not always available on an equal basis to all market participants, with elements controlled by some market players and/or technical providers. This control may result in some infrastructure being completely unavailable, while in other cases access may be restricted with particular terms and conditions. NFC antennas are an example. These are controlled by some players who can decide which kind of services and with which features can be accepted through these infrastructures and maintain the final say. Apart from setting the cost, they also decide other conditions such as reversing responsibility in case of fraud or imposing the authentication procedures. The ability of e-commerce platforms and app stores to decide on the means of payment or the lending provider that can be used in their infrastructure, instead of giving the users the capacity to choose, is another example.

It must also be considered that technical infrastructure providers can use their gatekeeping role to their advantage if they combine the technology provision with the supply of financial services.

As the trend towards greater digitalisation of financial services continues - and may strengthen in the wake of the COVID-19 crisis - it is essential that Europe has the appropriate foundations to enable competition and future innovation, underpinned by fair access to technical infrastructure. Some member states have started

to address these issues, such as Germany, who has introduced in their national regulatory framework an amendment in the German law implementing the Amended EU Directive 2015/849 (Gesetz zur Umsetzung der Änderungsrichtlinie zur vierten EU-Geldwäscherichtlinie) that obliges the controllers of the NFC systems to allow the access of other third-party payment apps to such antennas.

We therefore encourage the Commission to pursue EU level initiatives to avoid fragmentation in the Single Market caused by diverging measures on ensuring non-discriminatory access to relevant technical infrastructures supporting financial services.

Empower and protect EU consumers and investors using digital finance across the Single Market

An increasing number of new digital financial products and services expose consumers and retail investors to both opportunities and risks: more choice, more tailored products, more convenience, but also bad advice, mis-selling, poor information and even discrimination. Accordingly, it is important to carefully consider how to tap the potential of innovative products, services and business models while empowering and protecting end-users, to ensure that they benefit from a broader access to, and range of innovative products and services across the Single Market in a safe and sound manner. This may also require reviewing existing legislation to ensure that the consumer perspective is sufficiently taken into account. In addition, promoting financial education and digital financial skills may be important to ensure that consumers and retail investors are able to make the most of what digital finance has to offer and to select and use various digital tools, whilst at the same time increasing the potential size of the market for firms.

Question 24. In your opinion, what should be done at EU level to achieve improved financial education and literacy in the digital context?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
Ensure more affordable access at EU level to financial data for consumers and retail investors	○	○	○	◉	○	○
Encourage supervisors to set up hubs focussed on guiding consumers in the digital world	○	○	○	◉	○	○
Organise pan-European campaigns and advisory hubs focusing on digitalisation to raise awareness among consumers	○	○	○	○	◉	○

Collect best practices	○	○	○	○	◉	○
Promote digital financial services to address financial inclusion	○	○	○	◉	○	○
Introduce rules related to financial education comparable to Article 6 of the Mortgage Credit Directive, with a stronger focus on digitalisation, in other EU financial regulation proposals	○	○	◉	○	○	○
Other	○	○	○	◉	○	○

Please specify what else should be done at EU level to achieve improved financial education and literacy in the digital context:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The EBF is passionate about financial literacy and financial education as this is a basic requirement for any client. Without a basic level of understanding of personal finance, citizens are not able to make the right decisions that affect their long-term prosperity. Banks and the financial services sector note that a lack of understanding finances on the side of consumers/clients can ultimately pose a threat to financial stability.

Financial education arises as a complement to the financial conduct regulation and supervision of the financial system, contributing directly to the added value of the instruments regulating transparency and the duties of information of financial institutions and, consequently, to the more efficient functioning of the financial markets. Consumers who are “well educated” on finance, through their choice of financial products suited to their risk profiles and needs, help to promote a greater stability of the financial system by increasing sensibility around risks and towards financial inclusion.

Digital financial services bring new challenges to effective financial consumer protection in the digital era, in terms of both lack of familiarity with these new tools and low financial and digital literacy, including inadequate or insufficient awareness of consumers of how their data is used, and issues of transparency, disclosure and communication of terms and conditions. That is why more attention is needed to boost financial literacy. Effective actions require a collective effort from a broad array of stakeholders. The public sector can be in the lead, but – as experience has shown in a number of EU member states – all actors need to be represented.

Possible actions include:

- Cooperation among countries to develop consistent definitions of digital financial literacy and working together to increase recognition of importance of digital financial literacy. A significant effort is needed to include aspects related to financial literacy and digital skills in school and university curricula, to teach the financial basics.
- Technology based tools can contribute to raising financial literacy levels and can help individuals to make more informed financial decisions, as they improve accessibility and communication time with

customers. For example, the creation of digital platforms that present financial education programmes can be promoted. This could include an EU level digital platform where organisations can share relevant content.

- Promoting knowledge of the characteristics of certain products.
- New technologies allow remote workshops to be held to provide financial education to their different target groups, also other types of activities such as videos, online conferences, or open online courses. Digital tools should complement the financial education programmes acting as mechanisms to assist with communication and accessibility.

Ultimately, financial literacy is not only important in a digital context, nor it exclusively important in the context of a Capital Markets Union, as was suggested recently by the High Level Experts Group on CMU. As is also being advocated by the OECD, financial literacy needs to be recognized broadly as a critical life skill and has become even more important amid the emergence of a wide new range of digital financial services. In the digital context, financial literacy should clearly be linked to digital literacy programmes that address, for example, fraud awareness.

Question 25: If you consider that initiatives aiming to enhance financial education and literacy are insufficient to protect consumers in the digital context, which additional measures would you recommend?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

- Promote national platforms for financial education. These national platforms should include a wide range of stakeholders, including representatives of consumers, financial services companies, pension funds, banks, and Finance Ministries, Central Banks, Education Ministries and Economics Ministries. A good example of such a platform is Wijzer in Geldzaken, managed by the Dutch Finance Ministry. These platforms could be expanded to include representatives of emerging financial technology companies.
- Promote better educational systems so that citizens can be made better aware of possible problems stemming from the use of digital services. This could include for instance online gambling and online gaming.
- Cybersecurity is a critical aspect of digital finance. We recommend that cybersecurity initiatives such as those led by ENISA also are expanded to create room for discussion on personal finance aspects of the digital economy.
- At European level, funding from the Erasmus+ programme could be channelled towards cross-border educational initiatives that raise awareness on how financial services can be managed better in the digital context.
- Education technology can be used to gamify finance, which makes younger people much more engaged and receptive during the learning process. Digital literacy and skills like coding should also be a priority in school curricula.
- Including training procedures at the moment of the subscription of financial products or reception of financial services by digital means. Increasing the number of simulations (for investment, mortgages, etc.) can help users get comfortable without putting money on the line.
- Carefully consider the development, benefits, and use of metrics to measure customers' financial well-being. To be determined is if customers' financial health is related to the financing programmes that firms offer. Commonwealth Bank of Australia (CBA) has partnered with the Melbourne Institute of Applied Economic and Social Research to develop two measures of financial well-being: one is an online self-assessment tool that helps gauge how individuals perceive their own financial health; the other one determines more objectively the customer's financial health, based on their financial data.
- The degree of digital literacy is not uniformly distributed across countries and societies within them.

Supporting the media industry to develop new formats to attract large portions of the population (e.g. cartoons, quiz, tv series, etc) could be a good completement to digital initiatives and approaches.

• Financial education initiatives also need to address topics such as the availability and effective usage of mobile money, mobile banking, internet banking and data protection.

III. Promote a well-regulated data-driven financial sector

Data-driven innovation can enable better and more competitive financial services for consumers and businesses, as well as more integrated capital markets (e.g. as discussed in the on-going work of the High-Level Forum). Whilst finance has always been a data-intensive sector, data-processing capabilities have substantially improved over the recent years, enabling fast parallel computing at low cost. Large amounts of data have also become available as computers and their users are increasingly linked, supported by better storage data capabilities. These developments have enabled the use of artificial intelligence (AI) applications to make predictions about future outcomes at a lower cost. Following on to the European data strategy adopted on 19 February 2020, the Commission services are considering a number of steps in this area (see also the parallel consultation on the Mifid review).

Question 26: In the recent communication "A European strategy for data", the Commission is proposing measures aiming to make more data available for use in the economy and society, while keeping those who generate the data in control.

According to you, and in addition to the issues addressed in questions 27 to 46 below, do you see other measures needed to promote a well-regulated data driven financial sector in the EU and to further develop a common European data space for finance?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Under the PSD2 framework, banks already share a very important part of their data (payment/transaction data i.e. part of the banks' core customer data). As the PSD2 requirements to provide access to customer data only apply to banks and mandate this access to be for free, this has created a significant competitive disadvantage for financial institutions, particularly with respect to firms that are able to combine PSD2 data with their own non-financial data sources. Moving beyond PSD2 to include other financial products without also taking similar action in other sectors through the introduction of cross-sectoral data sharing, would deepen the existing data asymmetry faced by banks, preventing competition from taking place on an equal footing and limiting wider opportunities for innovation, which the European Commission's Data Strategy aims to create.

The greatest opportunities for data-driven innovation will come from reusing and combining data, particularly across sectors. This is being underscored by the current Covid-19 crisis (e.g. importance of telecoms or mobility data to address challenges in the health sector). As the Commission outlines in its Data Strategy, "making more data available and improving the way in which data is used is essential for tackling societal, climate and environment-related challenges." In the Strategy, the proposal for a Green Data Space shows

the importance of creating an ecosystem of data that is not limited to sectoral boundaries.

Most importantly, users should be at the centre of the data economy and regulatory initiatives should directly help individuals and firms to take control over their data in the digital environment - how it is used ,how it is shared and with whom, within the frame of user and firm data protection laws (GDPR and other national data protection laws; competition laws, intellectual property, business secrecy, banking secrecy, etc.). It is also important to help consumers to provide this access in a simple way, ensuring that it can be easily revoked when consumers choose, and that they are aware of and responsible for their choice.

A number of initiatives proposed in the Commission's Digital and Data strategies offer a practical first step towards achieving this. The Commission should focus on enhancing the existing data portability right under Article 20 GDPR through the Data Act so that it is actionable and practical. Recognising the complexities of implementing enhanced portability for all firms and datasets in the short term, the Data Act should focus on requiring enhanced personal data portability for a subset of organisations holding data of particular value to individuals. This should include data from:

- Digital platform providers (e.g. e-commerce, social media, streaming, mobility service). This could be done through introducing specific requirements regarding data portability under the ex-ante regulatory instrument for large online platforms.
- Telecommunications providers;
- Utilities (e.g. gas, electric, water); and
- Public authorities (such as public registries, tax, and social contributions data).

The Commission should also work towards a suitable data portability right for firms in a similar way to the inclusion of business accounts in PSD2 (ensuring this is designed to protect intellectual property and personal data rights). There is an opportunity to start with business user's data held in significant digital platforms under the planned ex-ante regulatory instrument.

Regarding the proposed sectoral data spaces, we understand that Data Spaces are a way of organising initiatives around key sectors and policy priorities and we support work to encourage data exchange and reuse. Yet, we would like to underline that data is especially valuable across sectors, also to create a future looking data driven financial sector. For example, data from a Green Deal Data Space could be used by financial institutions as they support their customers green transition, including to enhance climate change risk assessments or analyse green loans.

The Strategy already notes that the potential cross-sector use of data between sectors needs to be taken into account. This should be expanded, and the Data Spaces initiatives should start from the principle of making all data available on a cross-sectoral basis (with necessary controls and licensing wherever appropriate). As a result, the Commission should consider how the data spaces will interact with one another, and this should be an element of the upcoming horizontal governance framework for common EU data spaces.

We would also like to note that, as the data spaces take a sectoral approach, online platforms are not included in the initiative. This creates the risk that big technology companies will continue to benefit from data from other sectors, while continuing to act gatekeepers to their own data.

Facilitate the access to publicly available data in finance

Financial institutions are currently required to make public a wealth of financial information. This information e.g. allows investors to make more informed choices. For example, such data include financial reporting and non-financial reporting, prudential disclosures under the Capital Requirements Directive or Solvency II, securities market disclosures,

key information documents for retail investment products, etc. However, this data is not always easy to access and process. The Commission services are reflecting on how to further facilitate access to public disclosures of financial and supervisory data currently mandated by law, for example by promoting the use of common technical standards. This could for instance contribute to achieving other policies of public interest, such as enhancing access to finance for European businesses through more integrated capital markets, improving market transparency and supporting sustainable finance in the EU.

Question 27. Considering the potential that the use of publicly available data brings in finance, in which areas would you see the need to facilitate integrated access to these data in the EU?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
Financial reporting data from listed companies	○	○	○	○	◉	○
Non-financial reporting data from listed companies	○	○	○	○	◉	○
SME data	○	○	○	○	◉	○
Prudential disclosure stemming from financial services legislation	○	○	◉	○	○	○
Securities market disclosure	○	○	○	◉	○	○
Disclosure regarding retail investment products	○	○	◉	○	○	○
Other	○	○	○	◉	○	○

Please specify in which other area(s) you would see the need to facilitate integrated access to these data in the EU:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

First of all, we would like to stress that the most important principle is, as the questions refers to, any initiative that could be considered must fully respect that only data that is publicly available could be integrated in a potential system of integrated information. By no means information that is not publicly

available, already subject to disclosure, must be part of this. The financial sector is one of the most regulated and supervised sectors and as such is subject to information requests (regular and non- regular, regulated, and non-regulated) by supervisors. Information that is not subject to disclosure should not be shared as this could create risks such as giving a wrong signal to the market or providing a competitive advantage to others (e.g. information on clients). Any initiative should leverage on what already exits so that it does not impose additional obligations to entities.

Integrated access is a useful device as it results in less development and difficulties than each member state having individual access requirements.

Regarding the data mentioned in the table, to meet the targets of the Paris Agreement and the objectives of the European Green Deal, non-financial data only from listed companies is not sufficient. While all listed companies should be subject to reporting, the reporting should be extended to:

- All large companies. The criteria for banks should be modified to include banks with more than 250 employees and more than 5 billion in total assets.
- Companies from sectors with a high transition risk (for example mining, carbon, smaller utilities for material risks (e.g. climate only), regardless of the size.
- All remaining companies based on a simplified minimum reporting framework taking into account materiality, proportionality in a structured manner and possible gradual implementation (sectors with high risks first).

In terms of specific data that should be reported:

- More detailed requirements on environmental matters.
- Clear link to taxonomy (Harmonized data collection with a clear nomenclature to allow automatization; data collection templates for each economic activity).
- Standardized scenario analysis following TCFD for large companies in polluting sectors.
- Alignment of strategies with 2 degrees.
- Number of key KPIs aligned with the disclosure requirements that will be specified in the Delegated Act of the Taxonomy Regulation.
- Gradually, associated revenues and expenses of eligible products or activities and the associated sustainable assets (both as a percentage of the total).
- Greater focus on information and data related to societal aspects
- Governance issues as in TCFD.

More generally, the public sector holds huge amounts of data of wider economic, scientific, and social value. Some of this is already made available today: a selection of member states and institutions have created data sharing portals and started to increase the amount of data that is published. However, there is still much more that can be done. The EU has taken a step towards better availability of public data with the Open Data Directive. We encourage the Commission to be ambitious as it defines relevant high-value data sets and recommend the use of APIs for data exchange with the public sector, to allow secure, real time data transfer across different firms. We therefore recommend to include the specific data sets:

Geospatial data:

- Businesses and public services locations and activities
- Detailed cadastre data for business and household premises

Earth observation and environment

- Natural disasters risk maps
- Energy data: official certification of building efficiency

Statistics

- Economic indicators at high resolution level (spatial: census section; timescale: monthly)

Companies and company ownership
- Company registration information and public accounts
- Court information regarding companies, e.g. public case brought by state against a firm

Mobility
- Anonymised disaggregated passenger travel information on all public transport (i.e. travel journey for each transport customer, without other personally identifying factors).

As part of the European Financial Transparency Gateway (EFTG) project, the Commission has been assessing since 2017 the prospects of using Distributed Ledger Technology to federate and provide a single point of access to information relevant to investors in European listed companies.

Question 28. In your opinion, what would be needed to make these data easily usable across the EU?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
Standardised (e.g. XML) and machine-readable format	○	○	○	○	◉	○
Further development of the European Financial Transparency Gateway, federating existing public databases with a Single EU access point	○	○	○	○	◉	○
Application Programming Interfaces to access databases	○	○	○	○	◉	○
Public EU databases	○	○	○	◉	○	○
Other	○	○	○	◉	○	○

Please specify what else would be needed to make these data easily usable across the EU:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

To make the data more easily usable across the EU we recommend to:

- Help the re-user to identify the exact authority that is the holder of a specific set of data (one-stop-shop).
- Ensure that the request for data access is processed faster, within agreed deadlines.
- Be able to provide anonymization of specific data for concrete use-cases.
- Offer the possibility to process data within a secure environment, so that the user does not need to obtain a copy of the data.
- Clarify from the outset the legal rules on the purposes for which the data can be used.
- Standardisation on a machine-readable format, providing data via standardized APIs and, where relevant/applicable, as a bulk download.

We would also like to recommend actions in the area of ESG data. The availability of quality ESG data is currently rather limited, insufficient to comply with the envisaged legislative and regulatory requirements and expectations. When available, data is often difficult to compare and raises reliability questions. Moreover, ESG data by third party providers can also be inconsistent and expensive for small-size financial market players, researchers, or academia. With an increasing demand for ESG information induced by regulation as much as markets, the lack of quality ESG data may lead to a number of challenges, an unlevelled playing field and even competition concerns.

In this light, the availability of high quality and comparable ESG data should be regarded as an EU strategic infrastructure project and as a priority to advance the EU sustainability objectives, by enabling both the measures of the 2018 Action Plan on Sustainable Finance and those which will be proposed under the EU Green Deal. We understand a common European Green Deal dataspace to support the Green Deal priorities is already envisaged in the EU data strategy. It could be in this context that the EU builds or supports, based on existing solutions, a central European ESG data register that could:

- Collect periodically, with the help of new reading technologies, existing climate change mitigation and adaptation data of companies that publish non-financial statements under the Non-Financial Reporting Directive.
- Collect other available relevant information, ESG metrics and relevant data points
- Interconnect the relevant EU and MS databases collecting ESG information
- Enable to upload information to the register on a voluntary basis

Data should be collected in a central EU register and made available digitally to users of non-financial information, not only investors, but also lenders and other users free of charge or at reasonable cost in order to ensure that data are widely accessible across member states in an open source format. The EU should also open up its databases that collect environmental reporting data and make those re-usable for finance providers via the central register on a statistical basis, protecting the private information of individuals.

We would also like to share some recommendations as regards securities markets data, where there is an opportunity to improve the access to all public information generated by regulators and investments firms and related to EMIR, MiFID 2 (pre-trade and post-trade transparency, pre-trade documentation, Best Execution quarterly -RTS 27- and annually -RTS28-), as well as other trading venue information (prices,

quotes, transactions, volumes, outstanding interest, index compositions, historical series). We would like to flag in particular the following points:

• Regarding regulators and investment firms information, it is important to simplify the EU securities market data structure and make it easily accessible to all market participants, making the best out of the huge costs linked to the production of the information already incurred by investment firms.
• Regarding trading venue (TV) information, market data fees have significantly risen for the past two years, while one of the objectives of the European market infrastructure regulation was precisely to lower the cost of access to information. At the same time, there is no standard format to access TV information. The TV information, in our view, should be cheaper, more open, and standardised.
• On retail investment products, there is a need for consistency and streamlining to avoid additional costs and an administrative/operational burden.

Consent-based access to personal data and data sharing in the financial sector

The Commission is reflecting how to further enable consumers, investors and businesses to maximise the benefits their data can bring in the financial sector, in full respect of our European standards and values, in particular the European data protection rules, fundamental rights and security.

The revised Payment Services Directive marked an important step towards the sharing and use of customer-permissioned data by banks and third party providers to create new services. However, this new framework is limited to payment data held by payment services providers, and does not cover other types of data relevant to financial services and held by other firms within and outside the financial sector. The Commission is reflecting upon additional steps in the area of financial services inspired by the principle of open finance. Any new initiative in this area would be based on the principle that data subjects must have full control over their data.

Better availability and use of data, leveraging for instance on new technologies such as AI, could contribute to supporting innovative services that could benefit European consumers and firms. At the same time, the use of cutting-edge technologies may give rise to new risks that would need to be kept in check, as equally referred to in section I.

Question 29. In your opinion, under what conditions would consumers favour sharing their data relevant to financial services with other financial services providers in order to get better offers for financial products and services?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

There are three key prerequisites for customers sharing their data to financial services providers:

1. They first need to have trust and confidence in any data sharing ecosystem. This includes:
• Consumer consent and transparency: consumer's need to be in control of the action to share any data, with clear consent mechanisms, coupled with appropriate explanations from firms sending and receiving data as to what data is being shared and with whom. The information provided to consumers should be clear, comprehensive and serve their needs.
• Customers should be able to control and track the use of their data by providers more easily and conveniently and be made aware of the protections accorded to them (e.g. GDPR). All actors must ensure that privacy rules are abided at all times, also when considering any further use of such data.
• Security: a high level of security is crucial. There must be appropriate authentication mechanisms and

communication protocols that guarantee the integrity of the sharing process.

- Licensing: sensitive data should only be shared with firms that have an appropriate licence given as part of an authorisation regime. Other data that may be less sensitive may be subject to proportionate controls, such as registration of firms receiving data and use of appropriate security measures.

2. Customers need to be shown a clear value proposition that makes data sharing worthwhile (a use case in which they see value) e.g. in order to benefit from easier process such as simplified application routes or to gain access to certain features. For example, within the UK, consumers are becoming more accustomed to sharing their data and understanding the benefits of credit reference agencies, for example, with many consumers using their credit scores effectively. It is understood how the sharing of data through these mediums can provide insight and value of products and services to consumers.

3. Consumers must have at their disposal the practical tools or mechanisms to be able to share their data in a way that is user-friendly and safe such as APIs or so called consent-dashboards. As it stands today, consumers have very few such tools available to them outside of the financial sector. As a result, they are unable to share the majority of their data held in non-financial services firms with financial services providers that could be used to improve the products they receive or offer them innovative new products and services.

Finally, standardisation of APIs, data models, security processes and certain aspects of an effective user experience are key to ensuring that portability or sharing tools that empower users can be implemented cost-effectively and offers users the ability to share their data in a way that is easy, safe and in real-time.

Question 30. In your opinion, what could be the main benefits of implementing an open finance policy in the EU?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
More innovative and convenient services for consumers/investors, e.g. aggregators, comparison, switching tools	○	○	◉	○	○	○
Cheaper traditional services for consumers/investors	○	○	◉	○	○	○
Efficiencies for the industry by making processes more automated (e.g. suitability test for investment services)	○	○	◉	○	○	○
Business opportunities for new entrants in the financial industry	○	○	◉	○	○	○
New opportunities for incumbent financial services firms, including through partnerships with innovative start-ups	○	○	◉	○	○	○
Easier access to bigger sets of data, hence facilitating development of data dependent services	○	○	◉	○	○	○
Enhanced access to European capital markets for retail investors	○	○	◉	○	○	○
Enhanced access to credit for small businesses	○	○	◉	○	○	○
Other	○	○	○	◉	○	○

If you see other benefits of implementing an open finance policy in the EU, please specify and explain:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We only selected other benefits as "rather relevant" to emphasize that the benefits will strongly depend on how an open finance policy is implemented in the EU and whether the initiative is limited to data that is now held by banks instead of all the data that is useful in the financial ecosystem. This also applies to questions regarding the responsibilities between different actors. We have recognised several weaknesses and challenges in the revised Payment Services Directive. Hence, any new initiative in the area of data sharing should not be based on the PSD2 framework as such (e.g. data protection and security related issues must be carefully considered and solved for any future data sharing initiatives).
The Commission should take a cross-sectoral approach to data sharing. Customers should be given the opportunity to give access to their data from:

- All financial service providers.
- From technology providers in the financial context which accumulate data from financial interactions.
- From non-financial service providers who may hold relevant data for the provision of financial services.

Taking a cross-sectoral approach allows consumers to have an entire view of their arrangements, allowing them to understand and optimise their financial situation.

In our view, open finance must therefore be considered in the broader context of an Open Data Economy and should be part of a cross-sectoral initiative. We would therefore recommend to focus on data sharing across sectors, with the consent of users, for the maximum benefit for them and with mutual benefits for businesses. Potential benefits include more innovative and convenient services for consumers/investors, going beyond current value propositions, enhanced access to credit for small businesses and business opportunities for new entrants in the financial industry, but also for existing firms who prove value for consumers.

However, if the open finance initiative is limited only to bank data, this could prove an obstacle to these and other potential benefits. It would also put banks at a significant disadvantage (and exacerbate current asymmetries)while also holding back the development of a data driven financial sector in the EU, particularly if the pace at which this initiative is developed is quicker than the Digital Services Act's initiative to open data from online platforms. In this case, there is a high risk for financial system stability and competitiveness as regards large technology companies.

Question 31. In your opinion, what could be the main risks of implementing an open finance policy in the EU?

Please rate each proposal from 1 to 5:

	1	2	3	4	5	

	(irrelevant)	(rather not relevant)	(neutral)	(rather relevant)	(fully relevant)	N.A.
Privacy issues / security of personal data	○	○	◉	○	○	○
Financial exclusion	○	○	◉	○	○	○
Poor consumer outcomes (e.g. unfair pricing strategies)	○	○	◉	○	○	○
Misuse of consumers' financial data	○	○	◉	○	○	○
Business confidentiality issues	○	○	◉	○	○	○
Increased cyber risks	○	○	◉	○	○	○
Lack of level playing field in terms of access to data across financial sector activities	○	○	◉	○	○	○
Other	○	○	○	◉	○	○

If you see other risks of implementing an open finance policy in the EU, please specify and explain:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In general, and as outlined under question 30, the emergence of all the risks listed above strongly depends how exactly an open finance policy is implemented. An open finance policy could contribute to and accelerate changes in the structure of the financial sector, to its detriment. In particular, where an open finance policy is not implemented as part of a broader cross-sectoral framework to enable data sharing across different types of firms, this will place existing financial services firms at a disadvantage in terms of access to data, with possible impacts on future competition, European competitiveness and financial stability.

We also see significant risks with regards to market structure and competition. An open finance policy that requires financial services providers to provide access to data and infrastructure without similar policies in other sectors and without and without appropriate remuneration creates challenges through making different datasets available to different firms and regarding the sustainability of the underlying infrastructure and the resources available for future innovation.

A number of authorities and researchers have identified that these risks are likely to be especially acute in the context of the entry or expansion of large technology firms in financial services verticals, as open banking / open finance policies can play a catalysing role by accelerating entry into new business lines and opening up new risk vectors. In particular, the extensive existing datasets held by large technology firms

could be combined with data made available through open banking / open finance policies to provide an unfair advantage over other financial services providers, with this effect strengthened by technology firms' large user bases and roles as gatekeepers in the digital economy giving them leverage over the customer interaction. The FSB has highlighted (BigTech in finance, December 2019) that the use of open banking initiatives could reduce the 'stickiness' of bank deposits and have implications for incumbent banks' cost of funding and stability.

Costs and benefits have to be distributed equally across all market participants. An open finance strategy should thus be an integral part of a European data economy. Focussing only on the financial sector would entail the risk that some market participants or even sectors are put at a disadvantage because they have to share data unilaterally. To cover the costs for setting up necessary infrastructures some sort of cost recovery should be possible.

Open finance policies such as PSD2 can expand the ecosystem of providers with whom users are able to interact in order to access financial services. Where rules regarding responsibilities and liabilities are unknown, unclear, or undefined, this can significantly complicate the ease with which users can resolve any issues that may arise and receive any appropriate compensation. In many cases users may revert to their primary financial institution, even if the problem lies elsewhere, generating additional overhead and risks for those firms.

Another risk is the growing dependence among financial service providers vis-a-vis digital platforms and eco systems. The latter use data to generate leads and allow them to provide financial services as an intermediary with the consequence of disintermediation and a distortion of competition. Discrepancy between data sharing standards in the EU and other regions of the world (e.g. US, Asia) may also affect global competitiveness of European firms that should be taken into due consideration.

We would therefore recommend the Commission to be vigilant of further unlevelling the playing field and encourage them to work with full financial data access in mind: not only data from all financial service providers, but also data gathered by technology providers in the context of financial relationships and data gathered by other players across different sectors, which is useful for financial services.

Question 32. In your opinion, what safeguards would be necessary to mitigate these risks?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Most importantly, an open finance policy needs to be part of a broader cross-sectoral framework to enable data sharing across different types of firms. As mentioned above, users should be at the centre of this framework and the Commission should focus on enhancing the existing right to portability under Article 20 GDPR through the proposed Data Act and introducing portability requirements under the ex-ante regulatory instrument for large online platforms. For firms, the Commission has an opportunity to start with business users' data held in digital platforms through ex-ante rules in the Digital Services Act but should also work towards a broader portability right for firms.

At the same time, competition and financial sector authorities should carefully assess on an ongoing basis the effect of current and future open finance policies to understand their impact on market structure and its implications for competition, European competitiveness, and financial stability. In this regards, within the

financial space, we consider that it would be necessary that any new initiative which obliges financial companies to further open their data -would also involve online platforms.

Turning to the risks mentioned in the table above, a number of them are already recognised and addressed in horizontal and financial services specific legislation, as well as through appropriate actions by existing financial institutions. In some cases, open finance policies could lead to an increase in risk through the presence of new entities in the financial services market and the availability of new processes or operations to users. These risks would be effectively mitigated by applying the same principles and rules to new entrants or firms managing additional financial data as are currently applied to financial institutions.

We recognise the problem of unfair pricing strategies and misuse of consumers' financial data, for example. However, we think that this is a cross-sectoral issue across all businesses. It should be treated in a coherent manner following the evolving guidelines in the EU. If there were specific rules just for the financial sector, they could easily end up being contradictory with other rules imposed on the sector. Due to the sensitive nature of financial services data and operations, any sharing of financial data requires a robust regime to be in place, providing for appropriate rules on consent, transparency, security, and licensing / authorisations. In addition, open finance policies must ensure that the broader ecosystem remains sustainable and conducive to future innovation. The following issues
need to be addressed:

- Sustainability and innovation: Under the current PSD2 framework, account providers are unable to charge third parties for access to data or payment initiation. This results in a part of the financial markets infrastructure being provided without remuneration, undermining its financial sustainability. To address this, firms should be able to recover the costs associated with the implementation and operation of open finance infrastructure, such as APIs, through reasonable charges on the use of such mechanisms.

- Responsibilities and liabilities: clearer rules and coordination models are needed to allow firms to resolve issues that may arise, including inappropriate use of data or loss of data in one part of the ecosystem, or recovery of funds related to a fraudulent payment when the responsibility sits with a third party.

- Given the sensitive nature of financial data, customers must have absolute confidence in the security of their data, full control over the data being shared and the right to determine to which services and under what conditions their personal data will be used. The scope of the customer's consent must be clear and verifiable, particularly when it comes to what data is to be shared. The different issues regarding the possible withdrawal of the customer's consent, for example, also need to be considered.

Other safeguards to help mitigate the risks include:
- Using the right authentication model.
- Governance, including the operational and security risk management framework, the risk management and control models, and outsourcing.
- Risk assessment, including the identification, classification and risk assessment of functions, processes, and assets.
- Protection of the integrity of data, systems, and confidentiality, physical security, and asset control.
- Clear certification schemes for FinTechs or other data processors.
- Privacy and cybersecurity: APIs only provide access to those entities that have proved they have the means to protect privacy and cybersecurity.

Question 33. In your opinion, for which specific financial products would an open finance policy offer more benefits and opportunities?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
Savings accounts	○	○	◉	○	○	○
Consumer credit	○	○	◉	○	○	○
SME credit	○	○	◉	○	○	○
Mortgages	○	○	◉	○	○	○
Retail investment products (e. g. securities accounts)	○	○	◉	○	○	○
Non-life insurance products (e.g. motor, home…)	○	○	◉	○	○	○
Life insurance products	○	○	◉	○	○	○
Pension products	○	○	◉	○	○	○
Other	○	○	○	◉	○	○

If you see other financial products that would benefit of an open finance policy, please specify and explain:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A crucial point to consider is the level of data that is open and which data. The focus is on data generated by users in their interactions with different service providers and their ability to share that data with whom they choose. The enhanced or derived data generate by providers, which create additional value to the user-generated data should not be accessible. Firms build value on top of raw or observed data (e.g. through analysis, data validation) and should be able to retain and build on this value. As such, sharing of derived and inferred data should not in general be made mandatory.

We caution against the risk that initiatives compelling the sharing of inferred or 'non-raw' data could also inadvertently stifle innovation and competition. Inferred or derived data constitutes a crucial strategic and economic asset and is a strong element of competitiveness for companies. It therefore cannot be considered as freely and automatically accessible to third parties, as they need financial, technical, and human investments. Moreover, banks are often legally required to guarantee a higher quality of data (e.g. for Anti-Money Laundering, credit facilitation etc.). These processes create an additional layer of value on top of the

raw data that should be recognized and valued.

Data sharing in relation to competition law and intellectual property law should also be carefully considered. Data which constitutes trade secrets or other business sensitive information should not be subject to data sharing.

Question 33.1 Please explain your answer to question 33 and give examples for each category:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

As mentioned above, we recommend that cross-sectoral approach to data sharing. Open finance is only one part of the data economy and taking a truncated view risks missing out on the potential benefits for consumers and firms, as well as exacerbating the associated risks to financial stability and competition.

The new data eco-system offers precious opportunities as it enables firms to gain insights through new data sources, giving the opportunity to deliver improved products and services to consumers. For example, SME credit is fully relevant across issuing and acquiring across businesses. More data provides additional benefits to understand and provide support for SME businesses.

Question 34. What specific data (personal and non-personal) would you find most relevant when developing open finance services based on customer consent?

To what extent would you also consider relevant data generated by other services or products (energy, retail, transport, social media, e-commerce, etc.) to the extent they are relevant to financial services and customers consent to their use?

Please explain your reasoning and provide the example per sector:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

There is indeed a growing acknowledgment that relevant data from different sectors holds significant potential for financial industry innovation, competition, and consumer empowerment. It can help provide users with enhanced customer experience, better risk management, stronger security and fraud detection, better services, and convenience. The key driver for the use of data should always be the users' interests and empowerment.

It is important to note that the focus is on data generated by users in their interactions with all types of services providers. Users should have the option to decide which data to share and with whom, based on transparent and informed consent.

The combination of financial data with data generated by other services or products has great potential to further improve existing financial services or create new value propositions for customers around their financial needs and beyond. The specific relevant data varies with the concrete product or service and typically includes personal as well as non-personal data. Priority data that could contribute to competition and innovation in the financial sector includes personal data, such as:

- Data held in large digital platforms, e.g. e-commerce, social media, mobility services.
- Data held by utilities, e.g. energy and water consumption.
- Data held by public entities or services, e.g. tax and social security contributions and data from the Civil registry (vital records and family unit).
- Retail purchases e.g. purchase of transport related services (relevant for sustainability decisions and products).
- Data regarding the value housing company share or real property, real time accounting data.

An example of a potential use case of combining financial data with data generated by other services is green financing and investment opportunities. By allowing consumers or firms to share information about their energy use and details regarding their property, more providers could build specifications to facilitate green loans for renewable energy installation. A customer would share with the bank information held by their energy provider on their energy consumption and data on their property from the national cadastre. Such access and further use of data would take place in line with GDPR. In terms of the benefits, individuals and firms would be able to receive advice directly from their bank on whether it is in their interest to make an investment in renewable energy installation and how this could be financed. By easing the information and administrative constrains on individuals, much wider installation of independent renewable energy could be achieved, supporting the economy-wide energy transition.

Key data relating to firms (which could be prioritized in relation to developing a portability right for firms) includes:

- Data held in large digital platforms such as:
  - E-commerce - sales history, inventory, ratings, and reviews
  - Social networks - advertising data, customer reviews and connections

Search engines - advertising data

- Data held by utilities, e.g. energy and water consumption
- Data held by public entities or services, e.g. tax contributions and data from business registries

An example of a potential use case is improved SME credit assessment based on online sales. SMEs are increasingly using online channels to reach customers, including e-commerce platforms and other types of marketplaces. Research has shown that data from these platforms can complement existing credit information and improve credit modelling (BIS Working Papers No 779. BigTech and the changing structure of financial intermediation). Key data would include real time sales, inventory, customer reviews and so called “web sentiment” data. Through this data, financial institutions may evaluate the reputation/trust that customers have of the companies they interact with, as well as the relationship of each business to other businesses and/or private customers. SMEs would share this data directly with a financial institution, which would incorporate it into their credit analysis, potentially in real time. SMEs would be able to evidence the strength of their business and receive better access to finance more easily. In turn, a better allocation of credit to SMEs would support investment and productivity growth in the broader economy.

We would also like to note the importance of public sector data (mentioned above in question 27). The banking industry, as a user of public data (e.g. meteorological data for its insurance business), recognizes its potential for the development of data enabled financial service offerings.

Finally, in order to set the right incentives in an economic and competitive environment, any data sharing

framework must find the right balance and allow a fair split of the economic opportunities and costs between the data provider and the data receiver.

Question 35. Which elements should be considered to implement an open finance policy?

Please rate each proposal from 1 to 5:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N.A.
Standardisation of data, data formats	○	○	○	○	◉	○
Clarity on the entities covered, including potential thresholds	○	○	○	○	◉	○
Clarity on the way data can be technically accessed including whether data is shared in real-time (e.g. standardised APIs)	○	○	○	○	◉	○
Clarity on how to ensure full compliance with GDPR and e-Privacy Directive requirements and need to ensure that data subjects remain in full control of their personal data	○	○	○	○	◉	○
Clarity on the terms and conditions under which data can be shared between financial services providers (e. g. fees)	○	○	○	○	◉	○
Interoperability across sectors	○	○	○	○	◉	○
Clarity on the way data shared will be used	○	○	○	○	◉	○
Introduction of mandatory data sharing beyond PSD2 in the framework of EU regulatory regime	○	○	◉	○	○	○

If mandatory data sharing is considered, making data available free of cost for the recipient	◉	○	○	○	○	○
Other	○	○	○	◉	○	○

Please specify what other element(s) should be considered to implement an open finance policy:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We would like to note that the selection above is based on the assumption that an open finance policy is implemented as part of a broader data sharing framework (as recommended in our response to the previous questions).

- Mandatory data-sharing beyond PSD2 (as mentioned in the table) should be pursued only on a cross sectoral level and any new initiative should not be based on the PSD2 framework as such. Not taking similar action in other sectors would deepen the existing data asymmetry faced by banks and heighten the risks associated with it.
- Market participants should be able to agree on adequate compensation for access to data, in order to ensure sustainable financing and fair distribution of costs for maintaining the relevant technical infrastructure.

In case the Commission proceeds with these conditions in mind, we would like to stress the following points:

- Control has to be given to the user who decides whether to share data and with whom.
- Accessing any such data should not be done manually, but through APIs; to ensure data sharing is safe and useful for innovation purposes.
- Variety is what makes the data powerful, so cross-sectorial data sharing is critical to trigger disruptive innovation.
- Incentives have to be kept for players to invest in data processing, so data sharing should not cover derived of inferred data, just the observed data that the customer has generating in his interactions.

Support the uptake of Artificial intelligence in finance

Artificial intelligence (AI) can bring considerable benefits for EU citizens and businesses alike and the Commission is committed to support its uptake with appropriate frameworks and investment. The White Paper on Artificial intelligence details the Commission's vision on a European approach for AI in Europe.

In the financial sector, AI and machine learning solutions are increasingly applied throughout the entire value chain. This may benefit both firms and consumers. As regards firms, AI applications that enable better predictions can result in immediate cost savings due to improved risk analysis or better client segmentation and product price differentiation. Provided it can be achieved, this could in the medium term lead to better risk management and improved profitability. As an immediate effect, AI allows firms to save on costs, but as prediction technology becomes more accurate and reliable over time, it may also lead to more productive business models and entirely new ways to compete.

On the consumer side, the use of AI applications can result in an improved price-quality relationship of financial services, better personalisation and in some cases even in financial inclusion of previously excluded consumers. At the same time, AI may entail new risks such as opaque decision-making, biases, discrimination or loss of privacy.

The Commission is seeking stakeholders' views regarding the use of AI and machine learning solutions in finance, including the assessment of the overall opportunities and risks it could bring as well as the specificities of each sector, e. g. banking, insurance or investment services.

Question 36: Do you/does your firm already deploy AI based services in a production environment in the EU?

- (●) Yes
- ( ) No
- ( ) Don't know / no opinion / not relevant

Question 36.1 If you/your firm do/does already deploy AI based services in a production environment in the EU, please specify for which applications?:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

EBF members are deploying AI in the following applications (non-exhaustive):

- Credit and risk
- Audit and compliance
- Marketing, pricing, product management and sales
- Financial advice to improve the financial health of our customers (includes aggregation, categorization, account balance and cash management services)
- CRM Intelligence
- Internal Help Desk procedures
- Chatbots
- Research products using big data and AI
- Fraud control in payments and using AI to support AML, KYC, and cybersecurity
- Regulatory analysis

Question 37: Do you encounter any policy or regulatory issues with your use of AI?

Have you refrained from putting AI based services in production as a result of regulatory requirements or due to legal uncertainty?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

We have recognised certain challenges regarding regulatory requirements, which may indeed limit the use of AI and thus hinder innovation. These challenges are also meaningful from the point of view of the competitiveness of the European financial sector.

- GDPR: Questions arise regarding the development of AI and the GDPR. Notably, automated decision-making rules (and rights of individuals) under Article 22 of the GDPR, and a strict interpretation of it, may

hinder companies from embracing AI to provide better services and safer solutions, since significant manual processes may still be necessary. AI-based decision-making should be subject to oversight and control, but efficiencies may not be realised if human intervention in individual cases becomes significant. In this regard, the exemptions provided by Article 22(2) of the GDPR are welcome.

Uncertainties and challenges regarding certain GDPR principles (e.g. data minimisation, storage limitation, purpose limitation) and obligations (e.g. restricted collection of sensitive data) in regard to AI development (including data processing for AI training purposes), have also been flagged. Taking, for example, the data minimisation principle against the volume of data needed to develop accurate AI data analytics. This is particularly important as AI and Machine Learning (ML) techniques pose an opportunity to provide more accurate results than less advanced analytics techniques thanks to processing large volumes of diverse and quality data. As an example, using large samples of data is one way of reducing the risk of bias in the outcomes. Another is the purpose limitation principle, which requires that models developed using AI will not "recycle" information which may prove useful to provide more accurate analysis, if collected for other purposes, thereby limiting the possibilities of finding new insights on existing data. Some of these challenges are also recognized by the ROFIEG report under Recommendation 25.

Regarding training data, which is considered a critical pre-requisite for any AI-application or implementation in order to be successful, some members flag that financial institutions should be able to use their internal data sets generated from their own business as training data for the AI. At the moment, the financial sector is not able to take full advantage of customer-generated information, which is problematic from the digitalisation point of view.

EU Member States take different approaches to their implementation of GDPR, the intersection of these different approaches can present issues for the consistent deployment of models across the EU and therefore negate the benefits that can be obtained from EU wide data insight and analysis of such models.

- Intellectual Property: IP considerations can cause legal uncertainty. For instance, who should be the holder of the IP rights when a supplier provided an AI solution with the technical and financial support of a bank? Program code and techniques can be valuable commercial intellectual property: requiring protection and open to "inspection" only from entitled third parties (e.g., supervisory authorities).
- Global coordination: As the use of AI in financial services becomes a key focus for global and regional authorities, harmonisation of approaches is key. EBF members operate cross-border business, meaning that regulatory fragmentation imposes unnecessary cost and operational inefficiencies, which inhibits the realisation of benefits from technologies such as AI.
- Clarity on the supervisors' expectations regarding the use of AI for risk management and capital requirement calculations. Currently, the framework for the approval of regulatory models is demanding, and banks' experience in the past shows that changes in the model development methodologies can be costly and involve often lengthy approval times.

Finally, banks can also face challenges when it comes to the timing of bringing new services to market. Under the current regulatory environment, the results of an AI experimentation (in development or test environments) cannot easily be used in production environment. On the other hand, if a bank works directly in a production environment, it implies the need to be subject to strict rules deriving from industry specific regulations, risking slowing down the potential use of AI. As a result, future development of the regulatory context should give the opportunity to rapidly validate the results of AI experimentation, while taking into account all the inherent risks.

Question 38. In your opinion, what are the most promising areas for AI-applications in the financial sector in the medium term and what are the main

benefits that these AI-applications can bring in the financial sector to consumers and firms?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

For the banking sector, AI provides great opportunities to enhance customer interaction and experience, improve cybersecurity and consumer protection, strengthen risk management, and enhance the efficiency of banking processes.

Improved customer experience
AI can help to ensure that customers are empowered through innovative products and services stemming from the technology. 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, AI-supported automated services will bring a wide range of choice in terms of services offered and customization capabilities driven by better use of data through advanced analytics, for example:

- Offering contextualised, personalised products and experiences.
- Making more accurate credit-worthiness assessments.
- Providing better financial advice.
- Better protecting customers from fraud.

In addition, through the lowering of complexity and costs associated with some services (e.g. advisory services and credit provision services) AI can help lead to easier access to financial services and facilitate financial inclusion. For instance, it is expected that robo-advisor's main contribution will be bringing portfolio investment to client groups who previously had no access to it.

Enhanced efficiency
Thanks to process automation or semi-automation or a human-machine interaction, banks can reduce errors and costs and free resource that have a direct impact in the quality of services offered and an improved customer experience. For example, using Natural Language Processing (NLP) for Call Centre Financial Advisors.

Fraud prevention
The cost of fraud associated to non-cash means of payment can be quite high and the risk is only set to increase. As the digital space continues to evolve, fraudsters may take advantage of new system's vulnerabilities, people's lack of digital awareness, or situations such as Covid-19, which has seen a proliferation of scams. AI can provide great assistance in the detection of fraud and other suspicious activities that are linked to financial crime more generally. Having a more secure system means increasing trust in the bank for both clients and financers.

Increased cybersecurity:
The security needs of financial institutions are unique, as cybercriminals constantly target attacks at entities where they can experience the most financial gain. Meanwhile, consumers trust their institutions to protect their confidential information. By leveraging AI, financial institutions can automatically analyse massive amounts of data traffic to detect anomalies which may be threats. The more data that is analysed, the more effective AI becomes: developing familiarity with typical behaviour patterns and recognizing suspicious activity faster which leads to more efficient alert systems and threat remediation. Analysing high volumes of security data allows machine learning algorithms to anticipate future attack vectors based on existing data. With AI, banks can constantly improve their security posture.

Better risk management:
Data analytics contributes widely to a better internal understanding of banks' activities, a more effective risk management, and an improved monitoring of compliance. Financial institutions of all types, whether incumbent, challenger or digital-only, are investing great resources to deploy such services within the framework of already existing regulation, including, but not limited to CRD IV, MiFID II and the GDPR.

AI can also help in AML/CTF efforts. Rapidly evolving business and technology make conventional methods for AML/CFT inefficient and call for a more innovative approach towards the fight against crime. Properly designed machine learning algorithms and AI can help reporting entities monitor transactions by sorting through the enormous number of "alerts" and selecting only the critical ones. Machine learning will allow algorithms to identify patterns in criminal activity and update accordingly the screening filters of the tools in an agile manner.

Optimization of Sales and Marketing Processes
AI can help to optimize banks' sales and marketing processes, through dynamic personalization of content and an omnichannel customer experience and segmentation based on AI that short sales cycles, guided selling, and campaign cost optimization.

Question 39. In your opinion, what are the main challenges or risks that the increased use of AI-based models is likely to raise for the financial industry, for customers/investors, for businesses and for the supervisory authorities?

Please rate each proposal from 1 to 5:

1. Financial industry

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N.A.
1.1. Lack of legal clarity on certain horizontal EU rules	○	○	○	○	◉	○
1.2. Lack of legal clarity on certain sector-specific EU rules	○	○	○	◉	○	○
1.3. Lack of skills to develop such models	○	○	○	◉	○	○
1.4. Lack of understanding from and oversight by the supervisory authorities	○	○	○	◉	○	○
1.5. Concentration risks	○	○	◉	○	○	○
1.6. Other	○	○	○	◉	○	○

Please specify what other main challenge(s) or risk(s) the increased use of AI-based models is likely to raise for the financial industry:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

It is important to note that the use of AI technology to assist or execute certain process does not necessarily introduce another category of risk. In the banking sector, the “three lines of defence” model (business, risk /compliance, internal audit) sets a high standard in effective risk management and control and these principles apply irrespective of the techniques used and therefore encompass AI as well.

• Regarding the lack of understanding from an oversight by the supervisory authorities, some authorities have a good understanding of AI while others do not. This creates an additional challenge.

• The lack of skills is another challenge, and we encourage investment in and the development of programs to foster the skills and knowledge needed by data scientists, engineers, mathematicians.

• Access to quality and consistent data sets presents a challenge for AI adoption in financial services. Broad data sets are required to train models, and to ensure the benefits data-driven innovation can materialise.

Finally, the debate on ethical considerations continue as well as questions on how to integrate ethical considerations into the design of products and services. Ethics is subjective and varies between individuals, culture, and time. As a result, there are no easy answers to ethical considerations. There is also no commonly agreed definition of what AI is. We are therefore of the opinion that it is important for ethics standards to be technology-agnostic, to apply to all technologies alike and not set different standards for different solutions. We also recommend to continue reflections and discussions on ethical considerations at a global level, which are important, along with other initiatives, to help foster consumers’ and citizens’ trust in the technology.

2. Consumers/investors

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N. A.
2.1. Lack of awareness on the use of an algorithm	○	○	◉	○	○	○
2.2. Lack of transparency on how the outcome has been produced	○	○	◉	○	○	○

2.3. Lack of understanding on how the outcome has been produced	○	○	○	◉	○	○
2.4. Difficult to challenge a specific outcome	○	○	◉	○	○	○
2.5. Biases and/or exploitative profiling	○	○	◉	○	○	○
2.6. Financial exclusion	○	○	◉	○	○	○
2.7. Algorithm-based behavioural manipulation (e.g. collusion and other coordinated firm behaviour)	○	◉	○	○	○	○
2.8. Loss of privacy	○	◉	○	○	○	○
2.9. Other	○	○	○	○	○	◉

3. Supervisory authorities

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N.A.
3.1. Lack of expertise in understanding more complex AI-based models used by the supervised entities	○	○	○	○	◉	○
3.2. Lack of clarity in explainability requirements, which may lead to reject these models	○	○	○	◉	○	○
3.3. Lack of adequate coordination with other authorities (e.g. data protection)	○	○	○	◉	○	○
3.4. Biases	○	○	◉	○	○	○
3.5. Other	○	○	○	◉	○	○

Please specify what other main challenge(s) or risk(s) the increased use of AI-based models is likely to raise for the supervisory authorities:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Challenges include:
- Regulator's capability to assume AI models supervision at scale.
- Financial institutions will increasingly use internal models based on the use of AI. This may pose a challenge for supervisors which will have to respond to the demand from individual companies. The use of AI should not create a bottleneck for the approval process.
- Collaboration between relevant authorities (e.g. with data protection authorities), where an issue is relevant to the competence of multiple authorities so as to ensure that any guidance and expectations are consistent and not in tension/overlapping with each other. This is valid not only for AI, but in general for new technologies.

Further discussion would be welcome on supervisory expectations in relation to transparency/explainability of more complex models.

Question 40. In your opinion, what are the best ways to address these new issues?

Please rate each proposal from 1 to 5

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N.A.
New EU rules on AI at horizontal level	○	◉	○	○	○	○
New EU rules on AI for the financial sector	○	◉	○	○	○	○
Guidance at EU level for the financial sector	○	○	○	◉	○	○
Experimentation on specific AI applications under the control of competent authorities	○	○	○	○	◉	○
Certification of AI systems	◉	○	○	○	○	○
Auditing of AI systems	◉	○	○	○	○	○

Registration with and access to AI systems for relevant supervisory authorities	○	◉	○	○	○	○
Other	○	○	○	◉	○	○

Please specify what other way(s) could be best to address these new issues:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Existing regulation and guidance: We would encourage supervisors and policy makers to ensure the suitability (or lack thereof) of existing requirements on governance and risk management regarding the use of AI. This should first be assessed before any new measures are considered or introduced. We are of the opinion that new, AI specific legislation is not required and believe it is key to take into account the consequences that any rules could have for the competitiveness of European companies. However, guidance developed by competent authorities on how to apply existing requirements to AI use cases could help firms to effectively apply their obligations under different regulatory regimes. Potential guidance could, for example, address suitable levels of explainability or interpretability for certain use cases. Guidance should not be overly prescriptive, as this would be in friction with the rapidly evolving nature of AI-related technologies. Regarding the Commission's AI White Paper, please see the EBF consultation response.

- Supervisory authorities: We encourage policymakers to increase resources and training available for regulators, to ensure that they are capable of providing oversight and supervision of AI. Regarding the lack of understanding from and oversight by supervisory authorities, sandbox models should be encouraged as these can help authorities understand better the advantages, of AI applications for companies and consumers, how to mitigate potential risks, and reduce uncertainty to foster innovation. An example is the FCA TechSprint. This may also help address concerns highlighted in the AI white paper, such as on transparency and traceability, and how developing techniques to demonstrate explainability and causality in non-traditional AI Models are advancing.
- Regarding GDPR and AI development, the challenges need to be addressed in a pragmatic way. The GDPR is a principle-based regulation that relies on a risk-based approach. Legislators and supervisory authorities should understand the interactions among the principles and obligations set in the GDPR and the needs of technology developments, provide guidance (where needed) and assess compliance. Obstacles to the adoption of digital strategies in the financial sector should be removed. This is notably true as it relates to the position of Europe in the global AI field.
- Data: Improved conditions for the use and exchange of data, such as the creation of a sandbox and pooling of data, would facilitate experimentation and research partnerships with AI and cooperation across company/sector boundaries. Enabled by findings generated on a broader data basis and with the support of AI methods, suppliers could take advantage of market developments more quickly and better respond to customer needs and thus improve their innovative ability and competitiveness also on a global scale. Initiatives to enable cross-sector data sharing are also crucial.
- Transparency and explainability: We believe a risk-based approach, based on the impact of the outcomes of the system would be better suited in ensuring transparency and explainability. Different solutions could be more useful in different situations. This is also important in regard to accuracy as there could be situation where a trade-off exists between predictive accuracy of a model and the model interpretability. For instance, while a linear regression is typically easier to interpret, it does not have the predictive power of a neural net with millions of parameters, although its results will be harder to explain. However, should this mean that the neural network should not be favoured in some cases? E.g. in screening skin cancer, should the diagnosis be made by a single doctor with experience on maybe a few hundred

cases, versus a system that can access and analyse millions of diagnosed cases, only because one option can provide an explanation more easily? A risk based approach could help to address this trade off. The principle of technology-neutrality should also be followed; the use of AI should not increase explainability requirements per se.

Creating an attractive investment environment for AI in Europe is crucial. As a result, a regulatory framework that encourages innovation and does not hinder the use of AI, while ensuring a high level of consumer protection, is necessary. In this respect, the global view on regulation should also be taken into account and we encourage continued cooperation with a range of stakeholders on actions such as developing international standards. This will help to harness the opportunities of AI. Finally, there is a need to bridge the AI awareness, information, and education gap between industry and the public to support industry efforts to build AI-powered financial services. This could be done with the help of civil society. Managing accurate and thoughtful communication about the aims and limitations of the technology is critical for its adoption.

Harness the benefits data-driven innovation can bring in compliance and supervision

RegTech tools that are emerging across Europe can bring significant efficiencies for the financial industry. Besides, national and European supervisory authorities also acknowledge the benefits new technologies can bring in the data-intensive supervision area. Following on the findings of the Fitness Check of EU supervisory reporting, the Commission is already acting to develop a supervisory reporting that is fit for the future. Leveraging on machine learning technology, the Commission is mapping the concepts definitions and reporting obligations across the EU financial services legislation to identify the areas where further standardisation is needed. Standardised concept definitions and reporting obligations are a prerequisite for the use of more automated processes. Moreover, the Commission is assessing through a Proof of Concept the benefits and challenges recent innovation could bring in the reporting area such as machine-readable and machine executable legislation. Looking at these market trends and building on that work, the Commission is reflecting upon the need for additional initiatives at EU level to facilitate the uptake of RegTech and/or SupTech solutions.

Question 41. In your opinion, what are the main barriers for new RegTech solutions to scale up in the Single Market?

Please rate each proposal from 1 to 5:

Providers of RegTech solutions:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N.A.
Lack of harmonisation of EU rules	○	○	○	○	◉	○
Lack of clarity regarding the interpretation of regulatory requirements (e.g. reporting)	○	○	○	◉	○	○

Lack of standards	○	○	○	◉	○	○
Lack of real time access to data from regulated institutions	○	○	○	◉	○	○
Lack of interactions between RegTech firms, regulated financial institutions and authorities	○	○	◉	○	○	○
Lack of supervisory one stop shop for RegTech within the EU	○	○	○	◉	○	○
Frequent changes in the applicable rules	○	○	○	◉	○	○
Other	○	○	○	○	○	◉

Financial service providers:

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather relevant)	5 (fully relevant)	N.A.
Lack of harmonisation of EU rules	○	○	○	◉	○	○
Lack of trust in newly developed solutions	○	○	◉	○	○	○
Lack of harmonised approach to RegTech within the EU	○	○	◉	○	○	○
Other	○	○	○	◉	○	○

Please specify what are the other main barrier(s) for new Financial service providers solutions to scale up in the Single Market:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Other barriers include:

- The ability to test RegTech solutions is often lacking. In order to assess the value of a RegTech solution, there would be a need to test run over billions of transactions a day to identify potential capacity issues. While unit testing is generally possible, volume testing is often problematic.
- When trying to develop a solution, in the physical world, a bank could adapt to different situations in a

more flexible manner. Software, however, is not as flexible once written. More clarity and harmonization are therefore needed from the side of supervisory authorities so that a system that is working properly in one country is not deemed to be non-compliant in another. It is often difficult to interpret a regulation and translate it into a process and an IT change. The diffusion of rules on machine-readable by design could be a huge advantage to the uptake of RegTech and the ability to propose solutions that are "ready to use" and able to meet client needs, in particular for those banks operating in multiple countries (i.e. different languages, different regulators involved).

Finally, national laws and practices differ. This lack of harmonization in EU regulation often leads to information requirements that are duplicated or even inconsistent, and also acts an obstacle to the development of the RegTech market. The latter becomes even more important in a complex institutional environment like the EU, where financial institutions must report to both national and EU level authorities, in the financial and nonfinancial space.

Question 42. In your opinion, are initiatives needed at EU level to support the deployment of these solutions, ensure convergence among different authorities and enable RegTech to scale up in the Single Market?

- (●) Yes
- ( ) No
- ( ) Don’t know / no opinion / not relevant

Question 42.1 Please explain your answer to question 42 and, if necessary, please explain your reasoning and provide examples:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

It could be helpful to define a coordinated plan with member states and the main authorities through an open and transparent sector dialogue, with a list of coordinated actions to be accomplished. One action is exploring is harmonization regarding the regulatory requirements imposed to RegTech.

RegTech sandboxes could also be a useful tool to facilitate the development and uptake of RegTech solutions. However, a heavy-handed regulatory approach is not recommended.

Question 43. In your opinion, which parts of financial services legislation would benefit the most from being translated into machine-executable form?

Please specify what are the potential benefits and risks associated with machine-executable financial services legislation:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

In general, every part of financial services legislation that refers to regular reporting could benefit from being translated into machine-executable form. This includes:

- EMIR
- SFTR
- MIFID 2
- REMIT (energy derivatives)
- FRTB
- NPL
- MMSR
- STS

The part of financial services legislation related to control functions would benefit in particular, including on:
- Timely analysis of potential regulatory impacts;
- Updating internal documentation to avoid any inconsistencies;
- A single understanding of requirements facilitates consistent interpretation;
- Better performance of second level controls by using Big Data approaches.

Potential risks in regard to machine-executable financial services legislation include:
- The possibility that decisions taken without human intervention are more difficult to audit (for example, in case of use of machine learning).
- Fully automated processes may not have clear accountability.
- As the market is not homogeneous and financial services providers' technological capabilities differ, not everyone may be able to implement machine-executable reporting. As a result, two sets of regulation will be needed (machine-readable & language). This creates issues with regards to different interpretations and how to align them.

Financial services legislation is a broad and complicated framework. Translating it into machine-executable form only partially, covering only a very limited part of the framework, may not be beneficial from the RegTech point of view.

Question 44. The Commission is working on standardising concept definitions and reporting obligations across the whole EU financial services legislation.

Do you see additional initiatives that it should take to support a move towards a fully digitalised supervisory approach in the area of financial services?

Please explain your reasoning and provide examples if needed:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A harmonised and coherent approach to reporting will increase the quality of data submitted, help regulators assimilate the information, and enhance the ability to compare different data sets with each other. This

makes it crucial for authorities and the industry to work together to enhance the efficiency of data reporting. It also creates opportunities to engage with solution providers such as RegTechs, who are playing a crucial role in making regulatory compliance more efficient and effective while reaping the benefits of greater standardisation, integration, and automation in data reporting.
In order for banks and supervisors to automate reporting the requirements must be stable, consistent, and frequent enough to justify the investments in IT required for that automation. Standardization of the different reporting requirements in terms of definitions, scope, content, and methodologies is a must and is the main challenge during the last years.

Supervisory reporting requirements across different EU-level reporting frameworks are far from coherent, and it is one of the main problems causing unnecessary burden for reporting institutions. For example, definitions are inconsistent between different reporting streams. The practice in recent years has also been that different authorities come up with new reporting requirements instead of utilizing existing information. The result is a new layer of reporting where each authority and new report looks at the same activity that has already been reported with only a slightly different angle. These kind of duplicate reporting requirements should be avoided. Furthermore, there is a need for coordination and collaboration between the relevant authorities regarding the development of new reporting requirements. Better coordination and a collaborative approach would also be beneficial from the digitalisation point of view as it would enable the development of more intelligent and effective tools and services for reporting purposes. It should also be ensured that there are no legislative barriers to share relevant supervisory reporting data from one authority to another.

It is important to note that standardising of concepts and reporting obligations should be done in conjunction with, national, regional, and global authorities, wherever practicable. EBF members operate on a cross-border in nature and this is inherent in many of the requirements, and obligations, in reporting development and submissions today.
Furthermore, the conclusions from the 2018/2019 European Commissions' Fitness Check of EU Supervisory Requirements identified technology as one of the main areas for improvement with the reference to explore the benefits of technological developments (i.e. RegTech and SupTech) and the challenges that come with the use of new data technologies. We encourage the Commission to take follow-up steps on this.

We would also like to flag the following initiatives which could be taken:
- One topic that could be addressed is to define, for all sources of new regulations, the appropriate digital set-up in order to facilitate the use of AI solutions to be more efficient and effective in the process of new law monitoring.
- Where an authority requires market participants to submit structured data to a regulator and or authorised repository on a regular basis there is the opportunity for automation. The automation should be native to every step of the regulatory lifecycle from rule drafting, consultations creation and ability to consume responses in machine readable form, as well as the final rules. Beyond that, the current method of providing guidance via Q&A must have embedded machine readable clarifications. Finally, whenever a regulation is amended any structured data changes are published in a machine readable form.
- There is an opportunity to develop a new model for the codification and publication of documents so that parties who wish to receive them in an automated way can identify a document has been published, make a decision on its relevance to the consumer, classify the content of the document and then route it internally to the relevant internal stakeholders. The efficiencies, reduced risk and beneficial outcomes for the regulators and Market participants are self-evident.
- A less formal and more frequent dialogue between authorities and market participants would be hugely beneficial in reducing interpretation risk.
- There is also an initiative towards integration of regulatory reporting obligations of credit institutions. We support this initiative and see a lot of potential benefits if properly implemented.

Question 45. What are the potential benefits and drawbacks of a stronger use of supervisory data combined with other publicly available data (e.g. social media data) for effective supervision?

Should the Please explain your reasoning and provide examples if needed:

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Overall, the use of 'other publicly available data' would need to be appropriately defined by regulators to the extent that it was relied upon from a supervisory perspective, along with the purpose for which it would be relied upon. An important consideration would be the extent to which the information provided can be verified. Where this information was limited to verified information that derives from social media platforms owned and operated by the supervised entity, this may be appropriate. However, in this context, it is important to note that regulators are mandated to supervise legal entities, as opposed to brand presence. Social media channels may represent the global brand messages that may be misconstrued or out of context with reference to individual legal entities that sit within a global group.

Broader reliance on social media information outside of the social media platforms owned and operated by the supervised entity would need to be very carefully considered from an accuracy perspective. It may be very difficult to accurately verify the source and correctness of such information and to therefore justify relying on such information for supervisory purposes.

IV. Broader issues

Question 46. How could the financial sector in the EU contribute to funding the digital transition in the EU? Are there any specific barriers preventing the sector from providing such funding?

Are there specific measures that should then be taken at EU level in this respect?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The financial sector is shaken by change as technology makes rapid advancements, customer expectations rise, and new service concepts emerge. Business models have been adjusted accordingly. Hence, it is paramount that the contributions to the digital transition should be assessed from an all-encompassing perspective considering all the different digitalization activities in which the financial sector is engaging.

The EU financial sector is essential in funding the transition towards a digital economy in the EU through

actions such as:

- Providing finance to support EU companies' technology adoption and their adaptation to the challenges created by digitisation (re-skilling, new customers' expectations and demands, etc.)
- Providing finance to support the scale-up of EU business across the Single Market as well as funding entrepreneurial activity.
- Offering convenient, efficient, and affordable financial services suited to the needs of EU companies and citizens.

To fulfil this role, the EU financial sector needs:

- An enabling regulatory framework with no unnecessary burdens to the use of technology such as Cloud, AI and DLT.
- A level playing field that ensures that all players can leverage the opportunities from digitisation while guaranteeing an adequate control of risks to financial stability, integrity, consumer protection
- Access to data under fair conditions to promote not only a data driven financial sector, but data-driven innovation in the EU (as outlined in the Commission's Data Strategy).
- A true digital single market for financial services that guarantees that EU citizens are provided with the most convenient products and services, irrespective of their location within the region.
- No regulatory fragmentation, both globally and within the EU, to enable the EU banking sector to be competitive in the global landscape.

Question 47. Are there specific measures needed at EU level to ensure that the digital transformation of the European financial sector is environmentally sustainable?

5000 character(s) maximum
including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Sustainable development means consistent consideration of environmental factors in the different operations of the financial sector. The sector is already actively involved in climate action and cooperation to reach the goal of the Paris Climate Agreement and makes its biggest climate impact through its funding decision and therefore has an important role in steering investments towards sustainable targets. Best practices in this regard should be promoted.

Furthermore, there are synergies between the digitalisation of financial services and sustainable finance. The Commission should find ways to exploit those synergies by:

- Leveraging data richness to help agents better monitor and integrate sustainability considerations in their decision-making processes
- Financial agents and regulators and supervisors can also leverage data and scenario analysis for the successful management of financial risks around climate-related issues.
- Fostering technology adoption might help increase transparency and accountability around environmental policies and private investments (i.e. DLTs) or enable energy efficiencies and optimization of resources.

A stable regulatory and policy framework is needed to ensure adequate incentives. Such a framework should be holistic, encompassing all actors and ensuring a level playing field, building on existing practices and regulatory frameworks to avoid overlaps and be flexible enough to accommodate the financial and technology developments develop.

The creation at European Level of a digital platform containing information relating to corporate non-financial

reports could provide an operational tool for banks to consider environmental parameters when evaluating projects to be financed.

Additional information

Should you wish to provide additional information (e.g. a position paper, report) or raise specific points not covered by the questionnaire, you can upload your additional document(s) here:

The maximum file size is 1 MB.
You can upload several files.
Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

df9ad78e-897b-4ba8-ac66-459f32159027/EBF_041452_-_EBF_EC_Data_Strategy_consultation_response.pdf

Useful links

More on this consultation (https://ec.europa.eu/info/publications/finance-consultations-2020-digital-finance-strategy_en)

Consultation document (https://ec.europa.eu/info/files/2020-digital-finance-strategy-consultation-document_en)

More on digital finance (https://ec.europa.eu/info/business-economy-euro/banking-and-finance/digital-finance_en

Specific privacy statement (https://ec.europa.eu/info/files/2020-digital-finance-strategy-specific-privacy-statement_en)

More on the Transparency register (http://ec.europa.eu/transparencyregister/public/homePage.do?locale=en)

Contact

fisma-digital-finance@ec.europa.eu