26 June 2020
EBA Staff
EBA Regular Use

EBA response

EC consultation on the digital finance strategy/action plan

The EBA used the European Commission's consultation response tool to submit its response. However, the response is also published in Word format for ease of access. For background to each of the Commission's questions please refer to the consultation paper.[1] *A 5000 character limit (including spaces) was been imposed for the majority of questions.*

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.

The EBA identifies four main groups of obstacles potentially impeding the capacity of the European financial sector to fully reap the opportunities of innovative technologies:

1. Existing regulation – or the absence of regulation – resulting in outcomes that are not technologically neutral

Technological neutrality is about achieving the right balance between facilitating innovation, scalability and competition across the EU Single Market whilst continuing to achieve the central regulatory objectives of consumer protection, prudential resilience, market integrity and ultimately financial stability.

In simple terms this should mean that (i) the use of a specific technology is neither preferred nor prejudiced and (ii) regardless of the technology or business model deployed, activities presenting similar risks should be subject to similar regulation and supervision (i.e. an 'activities-based' approach to regulation and supervision, rather than regulation of the underlying technology). For instance, consumers should always benefit from the same standard of protection when accessing

[1] https://ec.europa.eu/info/consultations/finance-2020-digital-finance-strategy_en

the same products and services, regardless of who is providing the service. This does not mean that the 'entities-based' approach for prudential purposes should be disregarded. Rather, it should exist in parallel to the activities-based approach to ensure that combination of activities provided by an entity and aggregate risks are appropriately regulated and supervised, in particular from a prudential perspective taking account of the impact of businesses failing.

Applying this approach, throughout the EBA's work pursuant to the March 2018 European Commission FinTech Action Plan and the EBA FinTech Roadmap, the EBA has identified cases where existing EU regulation, or the absence of regulation may be:

- unintentionally impeding the roll out of technology-enabled financial services and products;

- hindering the scaling of activities across the EU Single Market to the benefit of consumers; or

- posing a barrier to new entrants.

Notably, the EBA has identified that significant divergences in conduct of business requirements and approaches to remote customer onboarding present potential impediments to the scaling up of activities cross-border, and result in firms struggling to navigate a patchwork of domestic requirements in order to roll-out digital solutions (e.g. for customer on-boarding). [2] These impediments need to be tackled in order to meaningfully improve the functioning of the EU Single Market for financial services whilst preserving an approach that enables local risk specificities (e.g. on ML/TF) to be addressed.

2. Areas of existing regulation that require clarification in their application to use cases involving innovative technologies in the financial sector

On the whole, the existing EU regulatory framework does not seem to impede the application of innovative technologies in the financial sector. However, targeted clarity and consistent interpretation of certain provisions could further facilitate the application of innovative technologies.

For example, the implementation of the GDPR has created a strong framework for the protection of personal data, but the use of artificial intelligence in the financial sector could be further facilitated through targeted guidance and consistent interpretation of provisions related to the use, processing and sharing of data for AI purposes (indeed, the EBA is currently working with the EDPB to help clarify aspects relating to the GDPR and PSD2). For more details, please refer to the EBA's response to Question 40. Similarly, although this consultation does not cover crypto-assets, as

[2] https://eba.europa.eu/eba-calls-european-commission-take-action-facilitate-scaling-cross-border-activity

referred to in the EBA's January 2019 report, the EBA notes the need for clarification around the applicability of existing EU law to crypto-assets. [3]

Additionally, supervisory practices and the overall ambit of EU regulation should be kept under constant review in light of fast-evolving technological developments in order to ensure that the EU framework remains fit for purpose (on which see further the EBA's response to Questions 11, 13, 21 and 22, including as regards the EBA's role in this context).

3. Divergences between Member States in terms of the acceptability and regulation of the use of specific technologies, which might hinder innovation and impede technological neutrality

Some divergences in approach between supervisory authorities as regards the acceptability and regulation of specific technologies (e.g. DLT, use of crypto-assets, AI etc.) in the context of the provision of financial services are impacting firms' capacity to integrate technological solutions into their businesses and across group structures.

The EBA has made some progress in addressing this problem. For instance, the EBA's Guidelines on outsourcing arrangements, which incorporated the EBA Recommendations on cloud outsourcing, have promoted consistency in the application of regulatory framework and supervisory approach, facilitating the use of this type of service. This greater convergence aids the roll-out of cloud computing; indicatively, the EBA has observed 12% growth in the use of cloud computing across the largest EU banks[4] following the implementation of the EBA Recommendations.

But in areas such as AI and distributed ledger technology, further efforts are needed to promote consistency in the acceptability and regulation of new technologies, not only within the financial sector but across industry sectors (for example, via guidance or principles-based regulation reflecting the nascent nature of many of these technologies and the wide range of potential use cases).

Additionally, EU frameworks for the regulation of new financial services supported by innovative technologies should be developed on a timely basis in order to ensure a common approach to the mitigation of risk on which see, for example, the EBA's January 2019 report with advice for the European Commission on crypto-assets.

4. Access to knowledge and expertise on innovative technologies

Building knowledge and expertise on innovative technologies can be challenging for supervisors and regulators.

[3] https://eba.europa.eu/eba-reports-on-crypto-assets

[4] EBA Risk Assessment Report 2019, https://eba.europa.eu/risk-analysis-and-data/risk-assessment-reports

Bridging knowledge gaps between the industry, supervisors and regulators on FinTech-related developments, and between supervisors, is essential in order to ensure that the opportunities and risks from new technologies can be identified at an early stage thereby enabling timely and consistent adjustments to regulatory and supervisory stances and effective supervision and risk assessment.

To help bridge supervisors on innovation-related issues, the EBA has established its 'FinTech Knowledge Hub'. Knowledge-sharing is also reinforced by our efforts to gather the latest trends in technology developments and supervision and share them widely to enable supervisors to ask the right questions in a constructive way, for example with reports on outsourcing to cloud service providers, the use of innovative technology for customer due diligence, and Big Data and Advanced Analytics (all of which are accessible via the Hub[5]).

The EBA has also established on a joint basis with the other ESAs a European Forum for Innovation Facilitators (EFIF) where supervisors and regulators can meet to share experiences, technological expertise, and their reactions to the latest technology and innovations as observed through their local innovation facilitators.

Nevertheless, existing initiatives should be strengthened and new initiatives - such as the establishment of cross-sectoral EU teams on topics cutting across all sectors e.g. AI, cyber security, e-ID, data protection – could be considered. Targeted training programs across the EU, technical workshops organised by relevant authorities (e.g. ESAs, EDPS, ENISA), and webinars could also be considered along with sufficient allocation of human and technical resources in order to build and foster knowledge and expertise on innovative technologies among consumers, financial institutions, supervisors and regulators.

The themes identified above are reflected throughout the ROFIEG report. However, they require even higher attention and greater urgency given the acceleration of financial activity to digital settings triggered by the COVID-19 pandemic.

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?

The EBA recognises that increased digitisation can offer many advantages for consumers as acknowledged throughout the EBA's response. However, as other respondents are likely to identify advantages, in order to help ensure balanced feedback, the EBA will focus on the main challenges consumers (and, in fact, any customers) may face as a result of the digital transformation of the financial sector.

[5] https://eba.europa.eu/financial-innovation-and-fintech/fintech-knowledge-hub

By way of main challenges (which are not ranked), the EBA identifies:

- *Data breaches and cyber-security.* Increasing digitalisation can facilitate easy access to financial services. However, consumers may be exposed to newer risks in comparison with traditional means of access, including increased risk of cyber-crime, fraud, misuse or theft of data and disruptions to service provision as a result of cyber-attacks. These risks may emerge if stringent security systems are not in place.

- *Financial exclusion.* As explained in the ROFIEG report, although innovation in the financial sector is typically viewed as contributing a net positive towards addressing the issue of financial exclusion, it is important to remain mindful of risks that may exacerbate exclusion.

  First, not all consumers have access to electronic devices such as computers and smart phones. As the financial sector becomes increasingly digitalised, efforts are needed to promote digital inclusion in parallel with efforts to provide other means to access financial services for those who may not have capabilities to use the internet or card- or mobile-based payment solutions. Second, new technologies, in particular AI, machine learning and Big Data offer the potential for a broader, deeper and faster analysis of large data sets, including "soft data" (e.g. harvested from social media) relevant to the assessment of, for example, creditworthiness. It will be important to ensure the appropriate oversight and regulation of applications of technology to ensure ethical use of data and avoidance of bias as further explained in the EBA's report on Big Data and advanced analytics.[6]

  Additionally, the EBA is of the view that financial education and digital and financial literacy should be a complementary tool to any regulatory policy on which see further the EBA's response to Question 24.

- *Transparency and disclosure of information.* Consumer detriment may arise from inadequate, incomplete and non-suitable formats for the provision of information to consumers through digital channels, resulting in consumers' informed consent not being guaranteed. The disclosure of pre-contractual and contractual information to consumers buying financial services through digital means should be adapted in order to focus much more on the presentational aspects to ensure effective transmission of information via these channels. More specifically, the form, prominence and timing of disclosures should be adapted to the specific product or service, the digital channel(s), and the consumer's device.

  The preliminary approach to this topic is reflected in the EBA's Opinion on disclosure to consumers of banking services through digital means published in October 2019. However, the EBA stands ready to work with the European Commission to strengthen supervisory

[6] https://eba.europa.eu/eba-report-identifies-key-challenges-roll-out-big-data-and-advanced-analytics

convergence in this field and thus help enhance the functioning of the EU (digital) Single Market.

- *Lack of definition of cross-border provision of financial services.* EU legislation lacks clear criteria for determining the location of where a service is being provided, which is key to determining whether there is cross-border provision of services and whether it falls under the freedom to provide services or the right of establishment. This lack of clear criteria is even more problematic when services and products are provided through digital means. As a result, consumers may not be aware of, or may be confused about, their applicable rights and protections.

  In July 2019, the EBA, together with the other ESAs, published a Joint Report on cross-border supervision of retail financial services, which highlighted the issues and encouraged the EU co-legislators to provide more clarity, especially in the light of the growing phenomenon of the digitalisation of financial services. Similar findings and recommendations were highlighted in the EBA report on potential impediments to the cross-border provision of banking and payment services published in October 2019. The EBA urges the European Commission to take urgent action in this area.

Question 3. Do you agree with the choice of [the following] priority areas?

1. ensuring that the EU financial services regulatory framework is technology-neutral and innovationfriendly;
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.

- **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:

The EBA refers to its response to Questions 1 and 2 by way of explanation of the EBA's answer to Question 3.

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:

Technological neutrality demands that we should not inadvertently prefer or prevent the adoption of a specific technology nor prefer or prejudice a specific business model or service provider, whilst still continuing to ensure that our regulatory objectives, such as consumer protection, prudential robustness, market integrity and financial stability, continue to be met (see further the EBA's response to Question 1).

On the whole, the EBA regards the existing EU financial services regulatory framework to be technologically neutral, albeit the framework must be kept under review to take account of emerging technology developments. However, the EBA has identified in its work cases where existing regulation – or the absence of regulation – may:

- unintentionally impede the roll out of new technology-enabled financial services;
- hinder the scaling of activities across the EU Single Market to the benefits of consumers; or
- pose a barrier to new entrants.

The EBA draws attention to its report on potential impediments to cross-border activity[7] which explains that the full potential of digital solutions has not yet been achieved in the EU, in part due to divergences in regulatory requirements and supervisory practices across the Member States which may undermine the functioning of the Single Market. Additionally, a number of relevant examples are reflected in the ROFIEG report.

In particular, the EBA identifies in its report a case for further harmonisation of consumer protection, conduct of business requirements and anti-money laundering (AML) and countering the financing of terrorism (CFT) measures. Specifically, the EBA observes in that report:

> *'*[d]*ivergences may emerge between jurisdictions in response to national specificities. However, in some cases, issues may emerge that, alone or in combination, may have negative unintended effects, potentially creating complexities that impede consumer choice and the cross-border provision of services, in turn hampering the functioning of the EU Single Market. In the context of consumer protection and conduct of business requirements, greater harmonisation at Level 1, particularly related to imposed in host jurisdictions disclosure requirements and the allocation of imposed in host jurisdictions responsibilities for the supervision of complaints handling, would be required to mitigate challenges faced by firms when seeking to provide financial services cross-border whilst maintaining high*

[7] https://eba.europa.eu/eba-calls-european-commission-take-action-facilitate-scaling-cross-border-activity

standards of consumer protection. Further analysis of materiality would be needed to conclude whether these differences actively hamper the provision of cross-border services. In order to facilitate and possibly enable the scaling up of services provision across the EU Single Market and ensure an adequate and uniform level of consumer protection across the EU, further harmonisation in the area of the conduct of business, and consumer protection requirements would be required, while still respecting national competencies and local market specificities.'

Additionally, the implementation of GDPR has set a strong framework for the protection of personal data, which could be clarified in certain cases to support innovation. In particular, when it comes to the use of AI in financial services, guidance on the applicability of the GDPR could further foster an innovation-friendly regulatory environment. Moreover, the right balance between the framework for access to, processing and sharing of data through the use of AI should also be struck in order to promote innovation and competition and establish a level playing field amongst actors while at the same time ensuring the ethical use of personal data. For more details, please refer to the EBA's response to Question 6.1.

The EBA's FinTech work has also exposed areas where supervisors have adopted different policies or stances that show an inadvertent bias towards the status quo, quite often stemming from a lack of familiarity with newer technologies and the opportunities and risks involved (the EBA's work in relation to outsourcing to the cloud provides a good example in this regard). Differing approaches, and sometimes a lack of knowledge, can pose a very significant barrier for the scaling up of new technologies (for instance, taking the case of a banking group with a presence in multiple jurisdictions receiving different answers when asking whether it could pilot blockchain for intra-group transactions). For this reason, the EBA is taking steps to promote greater consistency in supervisory stances through specific initiatives to promote knowledge-sharing between supervisors (e.g. the EBA's FinTech Knowledge Hub[8] and the European Forum for Innovation Facilitators (EFIF)[9]) and to promote common regulatory and supervisory approaches (e.g. by updating guidance and regulation as needed, for instance, in relation to outsourcing to the cloud). However, actions to strengthen these initiatives are strongly recommended (see the EBA's response to Question 14) and the EBA stands ready to play its part and would welcome further mandates in this area.

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

[8] https://eba.europa.eu/financial-innovation-and-fintech/fintech-knowledge-hub

[9] https://esas-joint-committee.europa.eu/Pages/Activities/EFIF/European-Forum-for-Innovation-Facilitators.aspx

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

The EBA is of the view that the principle of technological neutrality is, on the whole, sufficiently embedded in the EU regulatory framework within the scope of action of the EBA, albeit that continuous monitoring is required to ensure that any inadvertent obstacles can be identified and addressed on a timely basis (e.g. by avoiding the inclusion of paper-by-default requirements and reviewing the concept of 'durable medium').

The EBA has always been a strong proponent of the principle of technological neutrality and has always sought to promote this principle in regulatory and supervisory approaches, including in the area of consumer protection, with a view to ensuring a level playing field between (competing types of) financial services providers and to facilitate innovation.

As stated in the EBA FinTech Roadmap, technological neutrality and proportionality can be pursued via three main avenues. The first is when reviewing existing EU measures/developing new measures and during ongoing monitoring of regulation and supervisory guidance, typically designed at the entity rather than the activity level. The second is in the authorisations space generally and, in particular, in understanding how sandboxing regimes and supervisory discretions and levers to achieve proportionality in authorisation and regulation are working to create the space for emerging technologies and new delivery mechanisms while maintaining robust and consistent entry criteria. The third is the sharing of supervisory knowledge and experience in assessing, and responding to, new technologies, which is critical in promoting technological neutrality in the daily work of supervisors.

In any context, the EBA advocates for a high standard of consumer protection. This does not mean that the exact same rules must be applied across all distribution channels in order to achieve technological neutrality since they may need to be adapted to the specific features and risks of the products and distribution channels with the aim of assuring the same outcomes in terms of consumer protection. This may be particularly relevant in the case of the internet of things (IoT) applied to financial services. Customers can currently perform transactions very easily using wearable IoT devices, open bank accounts or access financial products and services via smart speakers which offer voice commands. In order to mitigate the potential risk of consumers not being provided with the required information or advice before purchasing a product, or suffering detriment from potential new privacy and cybersecurity risks, online scams or lack of transparency regarding how those products and services are selected by the intermediary, the EU regulatory framework should be continuously assessed to ensure it remains fit for purpose.

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?

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

N/A

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:

The EBA Risk Assessment Report 2019[10] presented the status of adoption of new technologies in large EU banks, noting that cloud computing, AI and biometric applications are already in use by more than 55% of EU banks[11] while DLT is still largely in development phase, used by around 25%

[10] https://eba.europa.eu/sites/default/documents/files/document_library/Risk%20Analysis%20and%20Data/Risk%20Assessment%20Reports/2019/Risk%20Assessment%20Report_November%202019.PDF

[11] Based on a sample size of 65 EU banks.

EU banks. Nevertheless, smaller banks, payment institutions, e-money institutions and other FinTech institutions may face certain challenges in complying with supervisory expectations, therefore affecting the adoption of new technologies.

Distributed Ledger Technology

Based on the EBA's analysis, the main challenges to the use of DLT relate to certain transparency aspects[12] as well as the multi-party network environment, including the governance framework that should be established for this purpose. For example, such a framework should require participants to define and agree on data aspects, processes, roles and responsibilities, and dispute mechanisms.

In addition, certain requirements of the GDPR appear to pose some challenges for the development of DLT, such as the right to be forgotten, which might not be technically feasible for the records/data stored on the nodes.

Moreover, in case of DLT cross-border applications, legal uncertainties may exist with regard to the applicable legislation, accompanied by uncertainties on the legal value of smart contracts (where applicable) and the lack of a clear applicable jurisdiction, as the DLT nodes could be located in different jurisdictions with potential for conflict of law issues. For example, a digitally signed contract might not be enforceable in all the relevant jurisdictions.

Furthermore, the EBA has observed a growing interest in the development of DLT-based solutions for the clearing and settlement of exchange-traded and OTC securities, which could benefit from removal of potential regulatory barriers for DLT to be fully adopted. In addition, the potential implementation of DLT might introduce prudential and conduct risks that are insufficiently addressed by the existing EU regulatory framework.

Cloud computing

EU banks consider cloud computing an important enabler for the implementation of their digital strategies, growth and competitiveness. Following the implementation of the EBA Recommendations on cloud outsourcing, an increase of 12% was noted in the adoption of cloud computing across the large EU banks. Nevertheless, further actions could be taken to strengthen the legal certainty for industry participants on the use of cloud computing in the financial sector and to facilitate adoption by smaller institutions, in particular by reducing the 'negotiation' gap in concluding cloud outsourcing contracts between small/medium-size EU financial institutions and big cloud service providers. Such actions could include the finalisation of the standard contractual clauses initiative, as per the European Commission's FinTech Action Plan[13] accompanied by

[12] For example, as regards whether obliged institutions using a public DLT should carry out due diligence procedures of miners or nodes executing a smart contract and receiving a small fee for that (gas) to comply with their AML/FT obligations.

[1313] https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf

adequate endorsement from the European Commission and the national authorities. This initiative could also promote the supervisory convergence of prudential supervision of financial institutions across the spectrum of the financial services market. Moreover, the potential oversight framework on third party providers (including CSPs) envisaged by the European Commission Digital Operational Resilience framework[14] could further alleviate these concerns.

In addition, the EU regulatory framework could be further strengthened to address the growing market concentration risk that may arise from large non-EU cloud service providers, as well as the potential dependency of EU financial stability on non-EU countries. In addition, such a framework could address the supervisory concerns on the practical performance of supervisory work in relation to the assessment of outsourcing arrangements with cloud services providers, when they provide cloud services to supervised financial institutions. For example, while the legal framework provides the supervisory authorities with access rights to the cloud service provider's business premises, including the full range of devices, systems, networks and data used for providing the services to the supervised financial institution, in practice competent authorities noted that 'conditional' or limited access is provided by some CSPs.

It is noted that even when CSPs provide unconditional access, more coordination, cooperation and supervision on an EU level might be needed, due to the market power and the cross-border nature of some CSPs. This raises the need for more coordinated supervisory action when CSPs operate in different Member States in order to ensure a consistent approach and share experiences/knowledge among the competent authorities.

Artificial Intelligence -> Please refer to Question 40.

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.

[14] https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf

Setting up dedicated observatories to monitor technological and market trends (e.g. EU Blockchain Observatory & Forum; Platform Observatory)					X	
Funding experimentation on certain applications of new technologies in finance (e.g blockchain use cases)				X		
Promoting supervisory innovation hubs and sandboxes					X	
Supporting industry codes of conduct on certain applications of new technologies in finance				X		
Enhancing legal clarity through guidance at EU level for specific technologies and/or use cases					X	
Creating bespoke EU regimes adapted to nascent markets, possibly on a temporary basis			X			

Other	○	○	○	○	○	X

'Other' has been indicated to note the benefits of EU regulatory perimeter expansion, for example, relating to crypto-asset activities (on which see further EBA's the response to Questions 12 and 22).

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:

The EBA is a strong proponent of the principle of technological neutrality in regulatory and supervisory approaches.

Technological neutrality is about achieving the right balance between facilitating innovation, scalability and competition across the EU Single Market whilst continuing to achieve the central regulatory objectives of consumer protection, prudential resilience, market integrity, and ultimately financial stability.

This means that, regardless of the technology or business model deployed, *activities* presenting similar risks should be subject to similar regulation and supervision (i.e. an activities-based approach to regulation and supervision). For instance, consumers should always benefit from the same standard of protection while accessing the same products and services, regardless of the service provider and regardless of the technology applied.

This does not mean that the '*entities*-based' approach for prudential regulation should be disregarded. It should exist in parallel to the activities-based approach to ensure that combination of activities provided by an entity and aggregate risks are appropriately regulated and supervised, in particular taking account of the impact across all business lines of the failure of that entity.

On the whole, the EBA considers that the EU regulatory framework is technology neutral. However, in order to ensure the regulatory framework remains fit-for-purpose, the EBA is continuously monitoring market developments and the application of the regulatory perimeter. For example, in 2020, the EBA will carry out work focusing on the role of digital platforms in financial services

provision with the specific objective of assessing whether emerging bundles of activity are regulated in a comparable manner and if existing approaches toward consolidated supervision remain fit for purpose and technology neutral. The EBA also draws attention to its response to Question 22.

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:

[*We do not respond to the table as we do not consider that any of the options for the answers are suitable based on the question asked.*]

	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						

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:

[*See comment above.*]

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:

The EBA has not provided a response in relation to the first part of Question 10 as we consider the question to be an insufficient presentation of the potential issues and do not consider any of the options presented in the table to describe suitably the situation.

However, by way of general remarks, the EBA notes that any firm intending to carry out deposit-taking, investment, payments or e-money services in the EU must first obtain the appropriate licence under EU law. Therefore, regardless of the identity of the provider of the service, the same regulatory requirements will apply to each firm holding the relevant licence type.

In order to ensure that the regulatory framework remains fit-for-purpose, the EBA is continuously monitoring the regulatory perimeter and, in 2020, will carry out work focusing on the role of digital platforms in financial services provision with the specific objectives of (i) assessing whether emerging bundles of activity are regulated in a comparable manner, (ii) reviewing consumer protection and conduct of business aspects (e.g. conflicts of interest management, disclosures, complaints and redress arrangements), interconnectedness and operational resilience aspects, and (iii) considering if existing approaches toward consolidated supervision remain fit for purpose and technology neutral.

Turning specifically to the impact of the application of new technologies and processes for the delivery of financial services on market, liquidity, operational (including conduct) and other risks, the EBA notes that it is quite possible that digital transformation may impact these risks (potentially increasing or decreasing risk depending on a wide range of factors such as scale of application, relevant market, consumer behavior, market concentration etc). However, this is not so much a factor of *who* is using the technologies, but rather *how* they are applied. For instance, it is well-recognised that the dynamics created as a result of technologies applied to facilitate faster payments necessarily allow consumers to make faster withdrawals with an impact for liquidity modelling. Therefore, as is the case for the regulatory perimeter, market developments need to be continuously monitored to ensure regulatory requirements are calibrated appropriately to mitigate any changed or new risks emerging from the application of new technologies.

For completeness, the EBA also draws attention to its response to Question 11 and the impact on incumbent institutions. In particular, the EBA notes that increased access to the financial services

sector by technology companies, either directly or by establishing group companies, may, in the short term, increase the number of participants in the financial sector. However, longer term, competition within the sector may be impaired if a very wide variety of financial and non-financial customer data is monopolised by a small number of market participants.

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?

[*We do not propose to respond to some risk factors as identified in the table for the same reason as stated for the table under Q10 and in view of the mandate of the EBA.*]

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					X	
Liquidity risk						
Misselling of insurance products						
Misselling of investment products				X		
Misselling of credit products				X		
Misselling of pension products						
Inadequate provision of information				X		

Inadequate complaint and redress process and management				X		
Use/abuse of personal data for financial commercial purposes					X	
Discrimination e.g. based on profiles				X		
Operational risk e.g. interrupted service, loss of data				X		
Other				X		

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:

The EBA notes that any firm intending to carry out deposit-taking activity, payments or e-money services in the EU must first obtain the appropriate licence under EU law. Therefore, regardless of the identity of the provider of the service, the same regulatory requirements will apply to each firm holding the specific licence type.

However, in order to ensure that the regulatory framework remains fit-for-purpose, the EBA is continuously monitoring the regulatory perimeter and, in 2020, will carry out work focusing on the role of digital platforms (see further the EBA's response to Question 10).

Referring to the question about other 'consumer risks', the EBA identifies potential issues stemming from:

- *Risk of market concentration*. Technology companies, and especially those that already have a large market share and customer base, could leverage this customer base and gain significant market share in financial services, which, may (albeit depending on a range of factors including the response of incumbent financial institutions and, for example, any collaboration or partnership with tech companies) result in less competition between providers of financial services and with consumers having fewer financial institutions with whom they could interact, less choices in terms of financial products and services, and potentially face an increase of prices.

- *Risk of over-indebtedness*. The increased relevance of technological companies and other suppliers applying innovative technologies to enable the increased and faster availability of consumer credit online may also imply, in the absence of appropriate safeguards and of harmonised licencing and supervisory regimes for non-bank credit providers (including harmonised loan origination and arrears handling framework), a risk of over-indebtedness of some consumers.

- *Risks of ineffective disclosures and mis-selling*. Consumers can currently perform (and are increasingly) carrying out transactions using wearable IoT devices, and open bank accounts or access financial products and services via smart speakers which offer voice commands. The EBA notes that the increased reliance on digital interfaces and the internet of things (IoT) for access to and use of financial services could create many opportunities but also could create additional risks for consumers in the absence of appropriate safeguards to ensure the effective disclosure regarding the suitability and risks of financial products and services. It is essential that the EU regulatory framework is adapted appropriately. The importance of identifying appropriate target markets and sufficiently testing products before launch is also emphasised in order to effectively mitigate the risks of customers being offered unsuitable products and services.

- *Other risks arising from digital interfaces*. As outlined in other parts of the EBA's response (see in particular Question 2), without appropriate safeguards, the increasing utilisation of digital interfaces to access financial services may expose consumers to increased risks of fraud, data loss and theft. Additionally, consumers may face challenges in identifying the relevant service provider and point of contact/applicable law in the event of complaint or need for redress.

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:

The EBA is of the view that technology companies have the potential to become significant competitors in the provision of financial services. The increased number of competitors in the financial services sector may bring several benefits to consumers but, at the same time, may result in some risks for them. Technology companies can further increase the current competitive pressure for current incumbents since some of these companies have significant investment capacity, technological knowledge and expertise, as well as scaling experience to provide services at lower costs in large volumes. Over time, this may erode competition within the sector and result in having fewer providers of financial services in the EU in the coming years, with less competition and with consumers having a more limited choice of providers for financial services and financial products. (The EBA has noticed so far, that technology companies have become more active in the payments market than in the banking sector, potentially leveraging the PSD2 and data sharing through application programming interfaces (APIs) to enter the payments market given their existing customer base, scaling experience and available technology tools.)

The potential use of consumer data, currently held by technology companies, for payment and banking services, and combined with other forms of personal and non-personal data may raise concerns. Although some practices are subject to EU regulation, such as the GDPR, the risks are still there and require further consideration.

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:

In accordance with the EBA's general tasks and functions, the EBA carries out continuous monitoring of the regulatory perimeter in order to ensure that the taking of credit and other risks is appropriately regulated and supervised. In the context of this work, the EBA has previously set out the rationale for common EU frameworks for the regulation of crowdfunding and crypto-asset activities[15] to ensure the consistent regulation and supervision of risks and to facilitate the scaling of these activities cross-border. However, the outcome of the most recent monitoring did not expose a need for adjustment of the regulatory perimeter at EU level for other FinTech activities.[16] In 2020 the EBA will be continuing its monitoring work, including in the context of digital platforms, and will report on the outcome of that work.

Please also refer to the EBA's response to Questions 1, 10 and 22.

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):

The EBA identifies four key challenges for supervisors:

1. maintaining visibility over financial activities that are (a) provided in a jurisdiction through digital means or (b) may exist beyond supervisors' regulatory perimeter (e.g. crypto-asset

[15] https://eba.europa.eu/eba-reports-on-crypto-assets

[16] https://eba.europa.eu/eba-publishes-report-on-regulatory-perimeter-regulatory-status-and-authorisation-approaches-in-relation-to-fintech-activities

activities), in order to assess if changes to the regulatory perimeter are needed and identify and monitor interconnectedness in the financial sector arising from dependencies on technology providers (e.g. third party technology providers, digital platforms etc.) at national, EU and global level;

2. identifying risks and coordinating supervisory actions where entities may be providing different types of financial and non-financial products and services (e.g. via digital platforms) in multiple jurisdictions and may (a) fall within the ambit of different sectoral supervisors (e.g. data protection authorities on the permissibility and use of public Blockchain applications handling sensitive personal data) and (b) be subject to different regulatory requirements and supervisory expectations (e.g. regarding remote customer onboarding). This poses a significant and growing challenge, particularly, with the increasing entry of technology firms and retailers to the financial sector and the need, among other things, for the close monitoring of, for example, 'tied sale' activity, in order to ensure consumers remain appropriately protected (including as regards the use of their data) and risks to competition and financial stability are mitigated;

3. securing adequate knowledge, skills and expertise when it comes to the supervision of innovative technologies, including for the purposes of assessing the acceptability of the use of technologies in the context of the provision of financial services and whether and when to update any supervisory guidance or regulatory requirements in accordance with the principle of technological neutrality as described in the response to Question 1 (noting, in particular, that presently there is limited EU-level regulation, guidance or other measures on the acceptability of technologies and appropriate supervisory/regulation expectations and requirements);

4. leveraging any potential coming from SupTech and RegTech and develop initiatives in a consistent, coordinated and timely manner across the EU and globally, including with a view to enhancing supervisory capacity over firms/groups with a multi-sectoral and multi-jurisdictional reach.

As noted above, supervisors face challenges in responding to cross-border innovative business models and the EBA highlights the need for further efforts on both a sectoral and cross-sectoral basis to support supervisors in horizon scanning and developing consistent and coordinated supervisory responses in accordance with the principle of technological neutrality as set out in the EBA's response to Question 1. Additionally, these horizon scanning efforts should be carried out on an inter-temporal basis, first to ensure that obstacles to financial innovation can be identified and addressed on a timely basis, and second to ensure risks are addressed on a consistent, effective and proportionate basis; together contributing to ensuring the regulatory and supervisory framework is technology neutral and fit for purpose in the digital age. In line with the EBA's core tasks and functions, the EBA carries out regular perimeter monitoring exercises. However, EBA would welcome further mandates in these areas in order to promote convergence of supervisory practices

and help rise to the challenge of continuing to monitor and supervise effectively a fast-evolving financial sector.

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:

The EBA highlights the important role of capacity-building initiatives for industry and supervisory authorities on understanding innovative technologies and the opportunities and risks they present, along with the appropriate regulatory and supervisory measures.

Further to the March 2018 FinTech Action Plan and the EBA's FinTech Roadmap, the EBA has taken a number of steps (both on a sector-specific basis and in coordination with the other ESAs) to support greater information exchange, knowledge sharing, coordination and cooperation between industry and supervisory authorities on FinTech-related issues. In terms of EBA-specific initiatives, this includes the establishment of EBA's FinTech Knowledge Hub and technology-specific training initiatives (e.g. impact of FinTech on business models, cloud, cyber etc.) - for cross-sectoral initiatives, see below on EFIF.

Going forward, the EBA considers there would be significant benefit in substantially expanding such initiatives – in terms of both ambition and frequency.

This would require additional resources and responsibilities, accompanied by increased funding, with regard to the role and activities of the EBA's FinTech Knowledge Hub, for example, to enable the EBA:

- to expand its capacity to monitor closely technological developments in the financial sector (e.g. by following more closely pilot initiatives in the financial sector within, and potentially beyond, the EU);

- to refine and formalise the EBA's function in identifying obstacles to the application of FinTech in the EU financial sector;

- to enhance technical capacity (for instance, via new recruitments and secondment arrangements) to focus in greater depth on technology developments and support dissemination of information about such developments with supervisory authorities;

- to act as a central point of contact on information and knowledge sharing through extending cooperation and coordination with a broader set of authorities (including financial sector supervisors, national central banks and potentially other organisations such as other disciplinary/sector-specific regulators) in order to facilitate the much-needed multi-disciplinary approach.

Additional funding could also be applied by the EBA to facilitate the gathering of best practices and trends on SupTech and promote/facilitate the (collective) development of selected SupTech use cases for the benefit of supervisory and regulatory authorities in the EU. The EBA could also act as a center for excellence and networking in this context and help instigate scalable SupTech across the Single Market.

Turning to the European Forum for Innovation Facilitators,[17] the EBA considers that the EFIF provides a good means for supervisors to share experiences on a cross-sectoral basis, aiding the identification of innovation trends, regulatory and supervisory issues that require a cross-sectoral position (so as not to prejudice the capacity of one part of the financial system, or industry sector, to engage a technology), and to monitor interconnectedness on a multi-disciplinary basis. More regular and formalised discussion of these issues (e.g. perhaps focusing on 'real life' use cases in order to facilitate in-depth discussion of potential regulatory and supervisory issues) within the setting of the EFIF and the regular publication of 'lessons learned' would be helpful to promote common understanding of opportunities and risks and to identify areas warranting clarification or regulatory change. Additionally, training and development initiatives can help support supervisors in capacity building. In turn, this enhanced knowledge and information-sharing can inform on a timely basis potential policy responses conducted in existing committee structures.

Additionally, the EBA considers that leveraging the EFIF's capacity to engage with EU-level non-financial sector supervisors and regulators (e.g. consumer protection, data protection and competition authorities) would be helpful to facilitate cooperation and common supervisory stances on the acceptability and parameters of use of technologies within and beyond the financial sector and avoid duplication of work. This could take the form of targeted working groups depending on the topic and case under discussion e.g. EDPB/EDPS and ESAs working group on the interaction of GDPR and AI in financial services.

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?

As the European Commission notes in the introductory text to the section of the consultation paper 'removing fragmentation in the single market for digital financial services', issues relating to a lack of consistency in the transposition, interpretation and application of EU financial legislation and divergent regulatory and supervisory attitudes towards innovative technologies pose potential obstacles to the Single Market for digital financial services.

The EBA brings particular attention to the recommendations set out in:

[17] https://esas-joint-committee.europa.eu/Pages/Activities/EFIF/European-Forum-for-Innovation-Facilitators.aspx

- the EBA report on potential impediments to the cross-border provision of banking and payment services[18] which calls on the European Commission to facilitate cross-border access, including via the update of interpretative communications on the cross-border provision of services and further harmonisation of consumer protection, conduct of business and AML/CFT requirements;

- the ESA report on the cross-border supervision of retail financial products,[19] which calls on the EU co-legislators to consider reinforcing the harmonisation of Level 1 provisions governing the marketing and sale of services and products, especially in the banking sector, and to provide more clarity on when activities carried out through digital means fall under passporting, due to the lack of definition of cross-border provision of financial services;

- the EBA Opinion on disclosure to consumers of banking services through digital means under Directive 2002/65/EC,[20] which contains proposals for the revision of the mentioned Directive regulating the distance marketing of consumer financial services, aimed at harmonising disclosure requirements for the marketing and provision of financial services via digital channels and hence facilitating the operation of the single market.

For completeness, the EBA also refers to its report on crypto-assets,[21] as well as its response to the European Commission's consultation on digital operational resilience (in particular on third party providers' framework), and the ESA Joint Advice[22] on ICT risk management and cyber resilience pointing to the need for the development of a common cyber incident reporting framework, albeit these topics do not fall within the direct scope of the consultation.

Furthermore, the EBA underlines the importance of an improved, at national and European level, dialogue between consumer protection, prudential supervision and data protection authorities to assess the potential opportunities that may arise for the financial system from the GDPR, including the provision of targeted guidance to the industry on the application of data protection rules and principles in the financial sector.

The EBA also places an emphasis on digital financial literacy (see further the EBA's response to Questions 24 and 25).

[18] https://eba.europa.eu/eba-calls-european-commission-take-action-facilitate-scaling-cross-border-activity

[19] https://eba.europa.eu/esas-publish-recommendations-on-the-supervision-of-retail-financial-services-provided-across-borders.

[20] https://eba.europa.eu/eba-publishes-opinion-disclosure-consumers-buying-financial-services-through-digital-channels

[21] https://eba.europa.eu/eba-reports-on-crypto-assets.

[22] https://eba.europa.eu/esas-publish-joint-advice-on-information-and-communication-technology-risk-management-and-cybersecurity

Question 16. What should be done at EU level to facilitate interoperable cross-border solutions or digital onboarding?

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					X	
Harmonise rules governing the acceptable use of remote identification technologies and services in the Anti-Money Laundering legislation	X					
Broaden access for obliged entities to publicly held information (public databases and registers) to enable verification of customer identities					X	
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)					X	
Facilitate the development of digital on-boarding processes, which build on the e-IDAS Regulation					X	

Facilitate cooperation between public authorities and private sector digital identity solution providers	○	○	X	○	○	○
Integrate KYC attributes into e-IDAS in order to enable on- boarding through trusted digital identities	X	○	○	○	○	○
Other	○	○	○	○	○	○

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

The European Commission has issued a Call for Advice to the EBA on the future AML/CFT legal framework. As part of its response, the EBA will provide advice on the harmonisation of customer due diligence (CDD) measures where possible, including the CDD measures in non-face to face situations.

In the meantime, the EBA makes the following observations:

- CDD entails more than the identification of the customer and the verification of the customer's identity. This is because the information financial institutions obtain through the application of CDD measures serves to inform their ML/TF risk-rating of the business relationship and determine the CDD measures financial institutions will take to deter and detect ML/TF. The ML/TF risk rating of the business relationship is determined by various factors, including the type of customers, the services/activities provided, geographies and delivery channels, which should be assessed by financial institutions in line with the ESAs Guidelines on ML/TF risk factors.[23] At onboarding, it also includes among other requirements a duty to obtain information on the nature and purpose of the business relationship, and a requirement to obtain sufficient information to enable meaningful monitoring of the business relationship and associated transactions including, for example, information about the source of a customer's funds and wealth. The type and nature of the information financial institutions need to obtain in this context will vary from one business relationship to the other in line with the risk-based approach enshrined in the AMLD and international AML/CFT standards. The integration of CDD elements into, for example eIDAS, could potentially facilitate interoperable

[23] https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-on-risk-factors-and-simplified-and-enhanced-customer-due-diligence

cross-border solutions but it will not be enough to fully meet AML/CFT objectives in all cases.

- The ESAs' 2018 Opinion on the use of innovative solutions by credit and financial institutions in the CDD process [24] stresses that the EU's AML/CFT framework is technologically neutral and sufficiently flexible to allow financial institutions to utilise technology and innovative solutions. In this Opinion, the ESAs recognised that technology and solutions used in the CDD processes are constantly changing and therefore the development of prescriptive rules is neither possible nor desirable albeit that greater harmonisation of the use of technology across the EU for AML/CFT purposes may be needed.

  Instead, greater efficiency will be achieved by harmonising CDD rules. In a report published by the EBA in October 2019 on the potential impediments to the cross-border provision of banking and payment services in the EU, the EBA notes that the flexibility enshrined in the AMLD in relation to the way financial institutions discharge their CDD obligations is not interpreted in the same way by all Members States when transposing the directive in their national legislation. This means that there are divergent approaches towards the identification and verification of a customer through digital means and the remote on-boarding across the EU with some Member States' laws being more rigorous and requiring customers to be physically present at on-boarding and others having more flexible approach.

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.

[24] https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf

Make the rules on third party reliance in the Anti-Money Laundering legislation more specific			X			
Provide further guidance relating to reliance on third parties for carrying out identification and verification through digital means, including on issues relating to liability					X	
Promote re-use of digital identities collected for customer due diligence						
purposes in accordance with data protection rules						X
Promote a universally accepted public electronic identity						X
Define the provision of digital identities as a new private sector trust service under the supervisory regime of the eIDAS Regulation	X					
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:

Directive (EU) 2015/849 sets out specific circumstances in which financial institutions can place reliance on a third party to carry out certain CDD obligations on their behalf. In the absence of a

common approach to CDD, and divergent transposition of the AMLD's third party provisions into the national laws of Member States, reliance on third parties can sometimes be difficult, in particular in a cross-border context. Greater harmonisation of CDD measures, as described in Question 16, is therefore likely to make a significant difference to the way financial institutions can rely on each other for CDD purposes.

In September 2020, the EBA will publish its response to the European Commission's Call for Advice, where it will set out how to limit the legislative divergence and enhance the effectiveness of the overall AML/CFT framework across the EU. As part of this, the EBA will also consider provisions of third party reliance, taking great care to ensure consistency with the guidance on digital identities published by the Financial Action Task Force in March 2020 and with a view to fostering convergence of practice as a way to support access to the provision of financial services both locally and cross-border.

In addition, the EBA also highlights recommendation 19 of the ROFIEG report which calls on the European Commission, in consultation with the EBA and other relevant authorities, to investigate potential models (including public and private sector and hybrid models) for efficient, robust and trusted digital identity verification in order to support cross-border activity on both the demand and supply side. This work should also encompass potential measures to support interoperability and security standards for the sharing and exchange of 'recognised' digital identities.

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.

With a view to supporting access to the provision of financial services both locally and cross-border the EBA is supportive of proposals to facilitate Digital Financial Identities and refers to its response to Question 17 regarding further exploratory work on different models for digital identities for use within and beyond the financial sector.

For the purposes of AML/CFT, it is important to ensure that financial institutions obtain sufficient data and information from the customer that allows them to develop a good understanding of their customer base by:

- identifying and verifying the identity of each customer;

- identifying and assessing the ML/TF risk associated with each customer;

- assessing the purpose and intended nature of the business relationship with the consumer;

- identifying and verifying beneficial owners, where applicable; and

- in certain circumstances, clarifying the source of the customer's wealth and funds.

However, as set out in the EBA's response to Question 16, the type and nature of the information financial institutions need to obtain to meet their AML/CFT obligations will vary in line with the risk-based approach.

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?

The mandatory use of common identifiers in reporting frameworks but also in all public information would allow to improve the quality of the data, reduce redundancy, enable data processing, aggregation and calculation, as well as assure the comparability between data from different sources and times. This would bring enormous efficiency gains processing together different kind of data and is absolutely indispensable on data analysis, providing the means to compare and achieve a wider overview of information that could influence decision making processes and allow for a quicker reaction when needed.

Focussing on AML/CFT:

A further increased use of Legal Entity Identifier (LEI) could potentially support the fight against money laundering and terrorist financing during both onboarding and subsequent monitoring of the business relationship and associated transactions to detect suspicious transaction and make the application of CDD measures more efficient.

However, the use of LEIs is not enough, of itself, to meet financial institutions' CDD obligations as the information contained in LEIs falls short of that required for CDD purposes and because institutions remain ultimately responsible for any failure to meet their obligations under Article 13 of the AMLD.

In September 2020 the EBA will publish its response to the European Commission's Call for Advice, where it will set out how to limit the legislative divergence and enhance the effectiveness of the overall AML/CFT framework across the EU. As part of this, the EBA will consider LEIs in the context of its advice regarding any future harmonisation of CDD obligations.

More generally, the EBA would welcome the opportunity to further support the European Commission's work in this area.

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?

As set out in the January 2019 joint ESA report on regulatory sandboxes and innovation hubs (innovation facilitators),[25] these schemes have considerable advantages in establishing proximity between industry and supervisors on innovation-related issues.

For firms, innovation facilitators can enable access to dedicated supervisory resources with specialist expertise in innovative use of technology and support firms in navigating the licencing/wider regulatory framework. This can be particularly helpful for firms seeking to enter the financial services market and for firms seeking to provide technological applications to regulated financial institutions and wishing to understand better the relevant requirements and expectations of supervisors.

For supervisors, innovation facilitators can enhance visibility of technology-related developments. This enhanced visibility can translate into a better and more timely understanding of opportunities and risks presented by innovations. For example, supervisors may react by building up supervisory expertise and resources in relevant areas, confirming and clarifying the application of the regulatory framework to financial innovations and, as appropriate, inform timely updates of regulatory and supervisory practices both to mitigate risks and address potentially undue regulatory barriers to financial innovation or technological neutrality. Innovation facilitators can also offer reputational benefits by signalling openness to innovation (albeit some potential risks have also been identified). The rationale for innovation hubs and regulatory sandboxes is elaborated more fully in the January 2019 report.

[25] https://eba.europa.eu/esas-publish-joint-report-on-regulatory-sandboxes-and-innovation-hubs

The EBA notes that since the publication of that report, a significant number of new innovation facilitators have been established (and are listed on the EFIF webpage) and several further regulatory sandboxes are likely to become operational in the course of 2020. The EBA also notes that other types of schemes, for instance, 'accelerators' have been established with similar objectives to innovation hubs. The precise approach adopted by the competent authority reflects, among other factors, the local market conditions, structure of supervision, and the resources available to the relevant authorities in the Member States concerned.

In order to ensure that innovative technologies can be applied at scale in order to maximise potential efficiency gains, it is vital that consistency of supervisory and regulatory stances is achieved across the EU. The EFIF is expressly intended to promote greater cooperation and coordination between national innovation facilitators with a view to promoting this necessary consistency. Further measures to strengthen the role and capacity of the EFIF in this regard are strongly encouraged (see further the EBA's response to Question 21).

Question 21. In your opinion, how could the relevant EU authorities enhance coordination among different schemes [innovation hubs and regulatory sandboxes] 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					X	
Facilitate the possibility for firms to test new products and activities for marketing in several Member States ("cross border testing")				X		
Raise awareness among industry stakeholders					X	

Ensure closer coordination with authorities beyond the financial sector (e.g. data and consumer protection authorities)	○	○	○	○	X	○
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)	○	○	○	X	○	○
Other	○	○	○	○	X	○

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

The EBA considers that the European Forum for Innovation Facilitators (EFIF)[26] is working well as a means to promote coordination and cooperation among national innovation facilitators to foster the scaling up of innovation in the financial sector. However, the EBA considers that the EFIF could be further strengthened to facilitate coordination and cooperation between the authorities on a 'real time' basis. This further strengthening should be based on a cost-benefit analysis of all the proposed improvements favoring those which offer most "value added" leveraging the EFIF's existing mandate.

In particular, the EBA sees benefit in better publicising and formalising the EFIF's role in:

- signposting how firms can reach innovation facilitators in relevant jurisdictions (many firms still face challenges in navigating the regulatory perimeter and identifying relevant innovation facilitators);

- identifying and communicating to the ESAs (and EC where appropriate) on a 'real time' basis potential obstacles to the implementation or the scaling up of innovative solutions identified in the context of innovation facilitators and arising from: (i) divergences in supervisory stances; (ii) regulation - this in turn can inform on a timely basis potential policy responses using existing structures (e.g. in the form of new or updated ESA guidelines or

[26] https://esas-joint-committee.europa.eu/Pages/Activities/EFIF/European-Forum-for-Innovation-Facilitators.aspx

technical standards or recommendations for new legislative initiatives in order to address potential obstacles to financial innovation);

- acting as an interface between industry and supervisors on innovation-related issues. In particular, the EBA sees benefit in merging the EC's Innovation Lab with the EFIF's industry outreach function in order to provide a single platform for exchanges on innovation-related developments, including via roundtables and workshops.

Targeted expert working groups, for example, established under the EFIF, could also be established to analyse and share knowledge about technology use cases and discuss supervisory/regulatory issues (e.g. an EDPB/EDPS and ESAs working group on the interaction of GDPR and AI in financial services).

The EBA also underscores the EFIF's ongoing role in supporting the consistent design and operation of innovation facilitators across the EU whilst respecting the responsibility of competent authorities to design and operate their innovation facilitators in line with their supervisory mandates, resources and needs of the local market.

Finally, the EBA also highlights the role of complementary initiatives to support coordination and cooperation and capacity-building, for instance the EBA's FinTech Knowledge Hub and technology and sector-specific training initiatives (e.g. on AI, RegTech, cyber risk etc.). More funding for such initiatives would be highly beneficial to enable greater frequency and participation by the widest range of authorities (including financial sector supervisors, national central banks and potentially other organisations such as other disciplinary/sector-specific regulators). Additional funding could also be applied by the EBA to facilitate the gathering of best practices and trends on SupTech and promote/facilitate (collective) development of selected specific SupTech use cases for the benefit of supervisory and regulatory authorities in the EU. The EBA could also act as a center for excellence and networking in this context and help instigate scalable SupTech across the Single Market.

The EBA stands ready to play its role in supporting further supervisory knowledge sharing on FinTech and SupTech initiatives, including via the EFIF, and would welcome further mandates in these areas.

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

N/A

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?

In its October 2019 report, the EBA identified a number of potential impediments to the scaling up of financial services cross-border, notwithstanding the existence of passporting rights.[27]

The first important challenge is the identification of when a digital activity is to be regarded as a cross-border provision of services. Although this is a crucial element in determining which regulatory and supervisory frameworks apply, currently, competent authorities and firms lack clear guidance on how to classify cross-border activity under the freedom to provide services or right of establishment.

The second challenge stems from areas of EU law that are not fully harmonised or are not yet covered by EU law. In particular, the EBA has identified issues related to authorisations and licencing (e.g. the absence of a common EU framework for crypto-asset activities[28]), and aspects of authorisation and ongoing regulation that are non-harmonised even in relation to services for which EU licence or registration regimes are provided (e.g. consumer protection, conduct of business requirements and anti-money laundering (AML) and countering the financing of terrorism (CFT)).

Left unaddressed these issues may impede institutions and other FinTech firms from providing banking and payment services cross-border within the EU. Therefore, as set out in the October 2019 report, the EBA recommends that the European Commission take action, including the update of its interpretative communications to support the identification of cross-border services taking account of the digitisation of financial services, the development of legislative proposals to further harmonise requirements relating to consumer protection, conduct of business and AML/CFT, and the further consideration of the need for other measures (e.g. guidance) to support a consistent approach to regulation or supervision of activities for which passport rights exist.

The EBA also encourages the European Commission to continue its work to assess the potential benefits of further extending the regulatory perimeter to confer passporting rights for new services where appropriate to facilitate cross-border activity whilst effectively and consistently mitigating risks. The EBA agrees that there may be benefit in carrying out an assessment of the non-bank credit sector to determine if there would be benefit in strengthening the regulatory framework to support cross-border credit provision whilst ensuring high standards of consumer protection and mitigating risks of regulatory arbitrage. Opportunities to scale up innovation across the EU could be far better embraced if the freedom to provide services would 'truly' enable companies to offer services digitally across the Single Market and the EBA stands ready to play its part in supporting the European Commission in assessing the need for any further extension of the EU regulatory perimeter.

Question 24. In your opinion, what should be done at EU level to achieve improved

[27] https://eba.europa.eu/eba-calls-european-commission-take-action-facilitate-scaling-cross-border-activity

[28] https://eba.europa.eu/eba-reports-on-crypto-assets

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	○	○	X	○	○	○
Encourage supervisors to set up hubs focussed on guiding consumers in the digital world	○	○	○	X	○	○
Organise pan-European campaigns and advisory hubs focusing on digitalisation to raise awareness among consumers	○	○	○	X	○	○
Collect best practices	○	○	X	○	○	○
Promote digital financial services to address financial inclusion	○	○	X	○	○	○
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	○	○	○	X	○	○
Other	○	○	○	X	○	○

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

The EBA is of the view that increasing access to digital financial services, and the use of innovative financial services, tools and applications (apps) could open up new opportunities for businesses and consumers, with the potential to improve the level of financial inclusion for consumers. Access to digital channels is a prerequisite for digital financial inclusion. However, risks also exist if increased access is not coupled with sufficient levels of digital and financial literacy at all stages of financial life. In particular the risk of exclusion from the provision of financial services of certain categories of consumers exists without such measures.

Digital financial services bring numerous 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 the value of their data, and issues of transparency, disclosure and communication of terms and conditions. Consumers are also potentially exposed to traditional risks, including not only the risk of miss-selling and fraud, but also new risks such as misuse of personal financial data, digital profiling, cyber-crime, such as phishing, hacking attacks and behavioral issues, such as excessive borrowing and risks arising from overly complex digital assets and services. The fast pace of the digitalisation of money and finance, together with the development of new products and services, requires continuous education to be fully understood by consumers (e.g. through paper and web-based training).

A higher level of digital and financial literacy would help consumers make effective use of digital financial services and make effective and responsible choices. It could involve enhancing consumers' understanding of opportunities, challenges and potential risks linked to financial innovation, in particular regarding AI, machine learning and Big Data, the use of 'seamless' online financial services, including via multi-purpose platforms, crypto-assets, and cybersecurity issues. Clear rules of conduct for financial institutions, combined with programmes of financial education for consumers, will increase consumer trust in financial markets and contribute to financial stability. In addition, the consumption of financial services through digital channels has been accelerated by COVID-19 pandemic. Accordingly financial educational programmes should be complemented by the programmes developing over-all digital competences.

Following-up on the publication of the EBA Fintech Roadmap and as part of its financial education mandate, the EBA published in October 2019 a factsheet to raise consumers' awareness when choosing financial services through digital channels. The factsheet includes tips that consumers should bear in mind before choosing a service or when concluding an agreement for a particular service. A similar exercise could be conducted by the EBA on other issues defined together with the NCAs. Other means of outreach could also be considered.

Finally, it is important to clarify that by way of responding to this question, the EBA interprets the wording 'best practices' that is used in the question to mean 'good practices', as often financial education and literacy initiatives are very much designed and tailored for consumers according to

their needs and national specificities, and successful practices in one jurisdiction are not easily transferrable to become equally successful practices in other jurisdictions.

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?

In March 2020, the EBA published its second Financial Education Report (FER) 2019/20. The FER is based on the EBA financial education repository and provides an overview of the numerous initiatives that competent authorities have undertaken in their jurisdictions, primarily during 2018 and 2019.

As mentioned in the conclusion of the FER, engaging stakeholders in providing joint financial education programmes is also part of a broader consumer protection objective to offer transparent financial products. A more robust, safe and transparent financial system needs also responsible consumers who are actively involved in improving their financial awareness. Financial education, initiatives, including those offered by public authorities and financial institutions (e.g. free online and data security training), can help consumers make informed decisions and promote the intelligent consumption of financial products and services. The aim should be not only to pass on knowledge and skills ('financial education'), but also to ensure that people are sufficiently financially literate to make the right decisions when managing their personal finances in the real world ('financial empowerment').

The EBA is committed to continuing its coordination of national financial education initiatives at European level in order to promote the effectiveness of financial education and the level of financial literacy and to help, inter alia, improve consumer protection and the responsible consumption of financial products and services. Financial education and financial literacy remain however, a complementary tool to any regulatory policy. The risks arising from overly complex digital assets and services would need to be supported by appropriate regulatory and supervisory initiatives to protect consumers. In addition, it is also the responsibility of the financial sector to make sure that digital tools are adapted to all categories of customers and allow them to receive the necessary information to make informed financial decisions.

In addition to financial education initiatives, the EBA is of the view that to protect consumers in the digital context, there are other measures that should be taken at policy level, including:

- to enhance the digital literacy of consumers. Some consumers do not have the digital knowledge and skills that are required to make use of digital financial services, and there is the risk that they end up being excluded from financial services. The provision of financial services through digital channels has been increased during the last years and this tendency has been accelerated by the COVID-19 pandemic. In addition, it is necessary to ensure good-quality and affordable digital connectivity to all consumers.

- to improve the disclosure of information to consumers buying financial services through digital means by adapting the presentation and provision of information to those channels and making use of the insights of behavioural economics.

- to provide a definition of cross-border provision of financial services at EU level. With the increase of digital provision of financials services, it is easier and more common to provide financial services across borders. Therefore, it is more urgent than ever to clearly define criteria for determining the location where a service is provided, which is key to determine whether there is cross-border provision of services and whether it falls under the freedom to provide services or the right of establishment. In turn, this is critical for determining the applicable consumer protection, complaints handling and dispute resolution rules. Greater clarity in this area is vital to facilitate the cross-border of services from both a demand and supply perspective.

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?

Where consumers have a high degree of clarity about the use to which financial services providers may put their data, and if the grounds for use are well-defined in accordance with a sound EU regulatory framework, they may favour sharing their data.

More specifically, consumers are likely to favour sharing their data where this would enhance the quality, range or tailoring of the product/service offering and where they would obtain a better insight into their financial situation. In addition, consumers are likely to be in favour of sharing their data if this would lead to cost savings for them, either directly from financial services providers or as a result of being offered targeted discounts with specific trading partners of those financial services providers, or where consumers can control and monetise the use of their data (for example, by watching advertising, recommending products or creating community content).

However, in order for consumers to favour sharing their data, in accordance with GDPR and cyber risk and operational resilience requirements, they would also require:

- to be informed, in clear, comprehensible and plain language, the purposes for which their personal data is to be collected and processed, with whom their personal data may be shared and how their data will be used, so that they can decide whether or not to give their consent;

- to have significant control of their personal data, for example by having the right to access their personal data and rectify inaccurate personal data, and by having the right to object to the processing of it;

- to be assured that financial service providers have in place robust and secure measures to prevent data breaches, cybersecurity attacks and fraud;

- to have the ability to change financial services providers without restrictions from their current providers and to transfer their data to a new or different provider;

- to be able to share their data in an easy and user-friendly way.

The EBA is of the view the use of consumer data is already subject to an extensive set of legal requirements on transparency, automatic profiling, data minimisation, purpose limitation, accuracy, confidentiality and accountability, alongside the additional requirements deriving from EU legislative acts that mitigate risks for consumers. The EU legislative acts include the GDPR (which is outside the EBA's scope of action), as well as the revised Payment Services Directive, the Payment Account Directive, the Mortgage Credit Directive, the Consumer Credit Directive, the Anti-Money Laundering Directive and the Unfair Commercial Practices Directive.

In order to ensure the EU regulatory framework remains fit for purpose taking account of market developments and trends, including with regard to the use of 'non-personal data', the EBA considers that the European Commission and co-legislators should continue monitoring these developments in the coming years and adjust the legislative framework when required to guarantee that consumers can benefit from sharing their data without facing new risks. This work should encompass not only applicable requirements but also oversight and supervision mechanisms and tools to ensure a consistent and effective application of the requirements.

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?

Based on our latest analysis, the most promising areas for AI-applications in the financial sector in the medium term are the following:

a) *RegTech/SupTech-related and process optimisation applications*, including ML/TF risk, fraud detection, customer on-boarding process, ongoing CDD process and other AML/CFT processes, data quality improvement applications and reporting compliance obligations.

b) *Customer Engagement and Customer Analytics*. The former is focusing on customer relationship management applications (e.g. use of AI in the loan approval process) while the latter on improving customer intelligence / customer insights, including dedicated analytics fed by customer interaction data (e.g. sales analysis, product analysis, network marketing analysis), raising important strategic risk considerations. For example, use of chatbots or conversion of customers' voice into text (through natural language processing) for automated analytics.

c) *Risk Management*, mainly in the area of risk scoring and risk modelling as well as cyber security management. Significant interest is observed in the use of AI for credit risk assessment and subsequently in credit underwriting where currently AI models are not yet serving as primary models.

Main benefits to consumers from AI-applications

- Potentially new/enhanced financial products and services tailored to consumers' needs and profile (more personalised service)
- Potential of financial inclusion via the use of alternative sources of data, which might allow customers to gain access to financial services that they could not access before (e.g. due to a lack of financial information)
- Potentially easier and quicker access to financial services
- Potentially better pricing of financial products and services

Main benefits to firms from AI-applications

- Development of new/enhanced financial products and services tailored to customers' needs in a timely manner
- Better understanding of customers' behaviour, preferences and needs
- Potentially enhanced customer satisfaction
- Potentially better detection of fraud attempts and cybersecurity issues, and in general useful compliance tools
- Potentially greater efficiency and cost savings, through automation and optimisation of processes mostly in support functions e.g. more effective compliance and monitoring tools, streamlined compliance processes
- Automatic assessment of upselling or cross-selling business opportunities

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				X		
1.2. Lack of legal clarity on certain sector-specific EU rules		X				
1.3. Lack of skills to develop such models				X		
1.4. Lack of understanding from and oversight by the supervisory authorities					X	
1.5. Concentration risks				X		
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:

Based on the EBA report on Big Data and Advanced Analytics,[29] the EBA notes that the increased use of AI based models can raise the following main challenges or risks for the financial industry (where many can be addressed by acquiring necessary skills and establishing appropriate governance):

- The increased use of AI-based models would probably bring wider use of complex and sophisticated AI-based models, which could be **more difficult to understand and explain** (maybe even for the AI developers). Their applications may not have deterministic behaviour and their outputs will be extracted based on a probabilistic measure, which might harm institutions themselves, the customers and/or other relevant stakeholders. Nevertheless, the ongoing academic research and appropriate supervisory guidance could alleviate these challenges in the medium-long term.

- Potential challenge on the **integration of AI-based solutions with existing legacy systems** that may raise ICT risks, such as risks to data security and protection, data quality, change management, and business continuity and resilience concerns.

- Another challenge is that AI-based models might result in **potential misconduct when financial institutions do not properly train their employees** (in all three lines of defence) to use and understand AI-based applications, including sufficient understanding of their

[29] https://eba.europa.eu/eba-report-identifies-key-challenges-roll-out-big-data-and-advanced-analytics

strengths and limitations. It is of upmost importance that the control functions, in particularly the Internal Audit function, possess the necessary skills to provide assurance on the reliability of the underlying algorithms and data.

- There is currently **a shortage of skills**, as it is not easy to find human resources with all the necessary knowledge and experience (e.g. in data science, business, IT, statistics).

- Another challenge is the **growing reliance on third party providers**, offering AI services which usually facilitated by the use of cloud services. In some cases, large cloud service providers offer AI services as 'augmented' services to their existing cloud solutions. This may further increase the risk of vendor lock-in and concentration risk. The latter can happen if many institutions use the same third-party provider, either for model development or cloud services, or if the models are trained using the same procedure and on the same data; in that case, they may advise the same action at the same point in time, which, together with the speed of accumulation of risks, could lead to financial stability risks. When models obtain decision autonomy, the risk of herd behaviour could increase.

- AI-based applications could possibly take on tasks that previously required human intelligence, therefore a challenge for institutions would be to ensure that the **outputs of these systems do not violate their ethical standards** (e.g. ensuring that models are free from bias and model outputs are not discriminatory), taking also into account the potential reputation impact. This moral obligation could go above and beyond the fulfilment of applicable legal requirements.

- Another challenge is to ensure the quality of the data to be used for the development of AI-based models as the maintenance of data quality is the basis for the responsible use of AI. Key elements of data quality (e.g. accuracy, timeliness, consistency, completeness) should be respected to limit the **risk of outputs being biased or not being sufficient** as the applications' behaviour depends significantly on the data used for training, testing and validation.

- Potential challenge could be institutions' **inability to clearly explain** to supervisors (as well as to their own board members) **the purpose of implementing AI-based models**, and thus indicating not having full awareness of the entire scope of their operations.

- Potential challenge in ensuring that **AI-based models are fit for purpose** (and that they have been so for a period of time), **appropriately selected, operated and validated** with adequate data integrity and avoidance of bias in models. In addition, potential over-reliance on AI-based models could raise certain risks as they can result in both de-risking practices and over-permissive practices.

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

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

Based on the EBA report on Big Data and Advanced Analytics[30], we wish to note that the increased use of AI- based models can raise the following main challenges or risks for customers/investors:

- The growing use of AI-based models can **influence decisions that affect customers** raising the focus on ethical considerations, in particular when models with decision autonomy will start to update automatically. Potential impact on institutions' reputational risk management should be also considered.

- Potential lack of trust on AI-based applications by customers/investors in case their outputs **violate ethical standards leading to possible mistreatment or harm** – directly or

[30] https://eba.europa.eu/eba-report-identifies-key-challenges-roll-out-big-data-and-advanced-analytics

indirectly – of customers because of the institutions' deployment of AI.

- AI-based applications could (inadvertently or otherwise) **exploit behavioural patterns or psychological biases that are harmful to the financial well-being of consumers**. To this end, due consideration should be given to the interest of the consumer in the design and approval of customer-oriented use of AI-based applications. Another risk might be that AI-based applications could (inadvertently or otherwise) **nudge consumers towards choices that are harmful to their financial well-being**.

- Attention should be paid to robo-advisors, that might, for example, favour investment funds with higher commission or do not avoid misselling.

- **Risk of financial exclusion** for consumers who do not have the data required or do not want to share such data. At present, institutions extract valuable information by profiling users, i.e. by collecting data related to their behaviour (e.g. consumption behaviour, payment timeliness behaviour). These alternative sources of data may be used by AI-based models to make automatic decisions (e.g. to accept or refuse a loan request) that could negatively impact the user and determine his or her access to the (financial) service proposed.

- Similarly, **profiling** could become so granular that the concept of risk spreading in prices for services in general among different customers could lead to prices becoming very high (exclusion) for customers who fall into riskier categories (sometimes regardless of their actions, for example if they are ill or disabled). Moreover, this can further reduce the capacity of consumers to compare offers.

- Risk of 'generic' customer consent for data processing, without allowing customers to make an informed decision and potentially being 'forced' into providing consent without no alternative, as a 'take or leave it' condition.

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	○	○	○	○	X	○

3.2. Lack of clarity in explainability requirements, which may lead to reject these models				X		
3.3. Lack of adequate coordination with other authorities (e.g. data protection)				X		
3.4. Biases				X		
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:

Based on the EBA report on Big Data and Advanced Analytics[31], we wish to note that the increased use of AI- based models can raise the following main challenges or risks for supervisory authorities:

- Potential lack of technical skills and expertise may deteriorate the adequacy and effectiveness of supervisory work when it comes to the use of AI and as a result, it may not support a technology neutral approach for the use of AI. Moreover, necessary skills to enforce good practices for AI are in large part not present in the regulatory community, which could make it challenging for supervisors to fully appreciate the new opportunities and threats, including adequate involvement of ICT experts.

- Potential lack of regulatory clarity and certainty can lead to limited use of AI-based models and reduced benefits from its use in cases where supervisors will not be able to provide guidance to institutions on how to implement AI-based models in regulated activities.

- Potential dependency on third parties from the provision of AI solutions. For example, smaller might not be able to afford in-house development. It remains to be seen if the regulatory and supervisory framework on outsourcing would be sufficient.

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

Please rate each proposal from 1 to 5

[31] https://eba.europa.eu/eba-report-identifies-key-challenges-roll-out-big-data-and-advanced-analytics

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

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

For the European Commission

In general, it should be noted that AI encompasses a broad variety of different methods therefore, a "one size fits all" approach may probably not be suitable for all the methods.

- **High-level AI principle-based framework**

The EBA believes that the existing EU regulatory framework provides sufficient basis for the use of AI in the financial services and therefore **we do not see the need of a new AI-specific regulation with prescribed requirements**, which might set at risk the desired balance between innovation and the stability of the financial system. Nevertheless, **a high-level AI principle-based framework could serve as an appropriate foundation for the wider use of AI in the financial services,** covering areas already listed by the High-Level Expert Group on Artificial Intelligence, respecting though and not contradicting existing financial regulation.

Such a framework could cover, alongside with sectorial guidance, ethics, avoidance of bias, fairness, transparency (explainability and interpretability), level of human involvement, security and accountability on AI-based applications. Please refer below to the 'Potential role and work for the EBA'.

- **Clarity on the interaction of GDPR and AI**

The GDPR has set a strong framework for the protection of personal data and has increased the focus on proper data governance frameworks and strategies. Nevertheless, when it comes to the interaction of GDPR and the use of AI in the financial services, **the EBA would recommend the development of sectoral guidance on data protection for financial services *or* the development of supplementary guidance to the industry on the interaction of GDPR and AI**. In particular, such guidance could include clarifications and consistent interpretation of related provisions of the GDPR that could further support the use of AI within the financial sector.

Following our recent analysis, a number of areas were noted, which may benefit from further guidance and consistent interpretation across the EU:

- Clarity on whether customers' information on publicly available data (e.g. social media) could be used for credit worthiness or product development purposes, accompanied by related conditions e.g. whether customer notification and consent are needed.

- Guidance on requirements and measures to be taken when personal data is obtained from third parties (e.g. performance of due diligence, customer consent).

- Given that AI models require real data for training purposes, clarity on the conditions that need to be met, covering whether process of personal data is allowed without a specific consent under anonymisation or pseudonymisation techniques as well as the timing and adequacy of customer prior consent if needed, taking into account that both the specific type of data and the specific target (purpose of the data processing) are unknown until the deployment into production.

- Guidance on specific conditions that need to be met to ensure acceptable anonymisation of personal data to allow data processing or data sharing.

<u>For supervisory authorities</u>

- **Obtain the skills, knowledge and expertise** to appropriately challenge AI-based solutions and identify potential risks. These can build on supervisors' strengths in oversight of risk in general, including ICT, governance and consumer protection risks.

- **Reconsider the profile of the future supervisor**, who could combine skills already present in the supervisory community with insights into the use of new technologies, data and ethical aspects.

- Consider the **internal use of AI** as a way to both reap benefits and, perhaps more importantly, increase understanding.

- **Intensify dialogue with the industry** and particularly engage timely in the development of potential industry AI standards to understand their quality and limitations as well as to learn from them.

- **Improve, at national and European levels, dialogue with the data protection authorities** to assess the potential opportunities and risks that may arise for the financial system from the framework of the GDPR.

Potential role and work for the European Banking Authority

- **Support supervisory authorities** in all the above, particularly in building knowledge and expertise on AI and facilitate intensive dialogue with the industry and data protection authorities.

Based on the upcoming initiatives of the European Commission, **the EBA could develop in the medium-term minimum supervisory expectations on data management (including data quality) and the explainability of AI-based models**. Supervisory expectations on the type and applications of AI models could remove any related ambiguity and bring more confidence in the development of proper AI solutions.

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

[*Answered in part only because we do not have data to comment from the perspective of RegTech providers (commercial stakeholders).*]

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	○	○	○	X	○	○
Lack of trust in newly developed solutions	○	○	X	○	○	○

Lack of harmonised approach to RegTech within the EU	○	○	○	X	○	○
Other	○	○	○	○	X	○

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

The EBA conducts semi-annual Risk Assessment Questionnaires (RAQs) among the largest EU banks, in order to collect information on the market trends in the banking sector. The spring 2020 RAQ included questions on RegTech aimed to better understand the current landscape and identify any barriers hindering the possibility to fully leverage innovative tools for regulatory compliance.

Responses from a sample of 50 EU (mostly large) banks have shown a significant interest in RegTech, as around 42% EU respondents reported to have implemented at least one RegTech solution. Banks have adopted a wide range of RegTech solutions aiming to automate compliance processes. In particular, the main areas of RegTech solutions are the following:

- anti-money laundering (e.g. digital identification and KYC);
- transaction monitoring (e.g. tools leveraging on artificial intelligence and machine learning to identify frauds);
- reporting;
- risk management;
- monitoring regulatory requirements;
- strong customer authentication.

In terms of the challenges faced in the development and implementation of RegTech solutions, 40% of EU banks reported the **'dependency on third party providers'** as the biggest issue. Furthermore, approximately one out of three respondents considers the following elements as challenges to the deployment of RegTech solutions:

- organisational mindset and internal culture (34%);
- adequacy of internal skills, expertise and resources (32%);
- management of third parties (28%).

The adequacy of external resources (18%) appears to be a minor source of challenge. Some respondents also reported challenges related to: (i) carrying out the due diligence on service providers, especially the ones located in non-EU countries; (ii) fully understanding algorithms and the whole tech-process behind the proposed solutions; (iii) assessing the risks linked to the use of such RegTech solutions; and (iv) gathering quality data. In the EBA's view this may indicate that further work might be needed in the scope of application outsourcing requirements.

Interestingly, the legal environment in general (28%) and the specific **regulatory approach,** including the approach by and expectations of regulators and supervisors (24%) are indicated as another challenge in the implementation of RegTech solutions. This confirms our recent observations that **the existing EU legal and regulatory framework may pose some challenges in the deployment of RegTech solutions but it is not the main barrier to scale up RegTech solutions in the Single Market.**

As an example of regulatory challenges, several respondents pointed out the high level of complexity and continuously evolving nature of the regulatory landscape, which hinders the possibility to rely on RegTech solutions for regulatory adherence. Acquiring and implementing RegTech solutions in the existing infrastructure is typically costly, therefore financial institutions need to have certainty that investment will serve the purpose for the longer term. For example, Natural Language Processing tools are not currently able to substitute a manual horizontal legislation tracking process and a lot of expert-based work will continue to be required to properly scan the regulatory horizon. Moreover, a few respondents also underlined the difficulty to balance and reconcile competing (and sometimes conflicting) regulatory expectations of how data should be captured and managed (including GDPR requirements), often dependent on the country and interpretation of the legislation/regulation. Please also refer to our response in Question 6.1.

The lack of harmonisation in certain areas of regulation has been identified as a barrier for the scale up of innovative solutions also in the *EBA Report on potential impediments to the cross-border provision of banking and payment services*. For example, reference is made to the existing domestic restrictions to remote customer on-boarding and to the outsourcing of certain AML-related tasks (e.g. ongoing monitoring of customers and sanctions screening).

Finally, in the EBA's view, other factors that might constitute a barrier to the scale up of RegTech solutions are:

(a) the circumstance that many financial institutions, especially smaller ones, are still unfamiliar with RegTech possibilities, reliability, and acceptance, due to the limited track record of most RegTech solutions. This impedes procurement procedures;

(b) financial institutions' legacy systems and procedures, which might impede the smooth and quick integration of RegTech solutions.

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:

RegTech, if properly facilitated and implemented, can play a significant role to increase, first and foremost, compliance effectiveness, but also contribute to a greater efficiency.

To give a few examples, deployed RegTech solutions could increase effectiveness of AML/CFT processes (e. g. better data quality, reduction in human errors'). In addition, in the environment where banks' profitability is forecasted to be negatively affected by lower volumes, higher credit risk, and reduced fee and commissions income, resource-intense and costly tasks can be an additional drag for institutions that are still highly reliant on manual workflows.

Thus, an EU-wide cooperation is important to ensure that the legal and regulatory environment: on one hand, facilitates the scale up of RegTech at EU level, fostering the development of solutions which might provide benefits to the financial sector, in terms, for example, of effectiveness of risk management and efficiency; and, on the other hand, addresses the potential risk which may arise from the use of such solutions. We see that the EBA and the European Forum for Innovation Facilitators (EFIF) can play a very important role in this field.

In particular, EFIF can focus on identification of RegTech use cases in the EU financial sector, regulatory and supervisory issues arising and experience acquired by the competent authorities, with a view to promoting a common approach to the use of RegTech and supporting interoperability.

EFIF can provide a good overview of technology trends and use cases and major regulatory and supervisory themes, including any areas in which:

- common views on the appropriate regulatory and supervisory response are reached;
- recurrent regulatory obstacles or gaps impeding the scaling up of financial innovation are observed that may warrant attention by the ESAs and/or European Commission;
- recurrent risks with reference to the use of RegTech solutions are identified;
- analysis of the effectiveness of RegTech solutions to achieve AML/CFT goals compared to more traditional solutions is conducted; and
- policy action may be needed.

The EBA is well placed to conduct deeper analysis on selected RegTech use cases and issue an opinion on legislative changes needed to support the uptake of RegTech solutions. The EBA has already started investigating the use of RegTech in the financial sector, aiming to release its findings in early 2021.

RegTech initiatives at EU level could focus to facilitate financial institutions' engagement with third party (RegTech) providers to i) aid the screening process, ii) reduce the costs of 'due diligence', and iii) provide additional assurance of the quality of the services provided.

In practice, this support could take the form of:

1) [*short term solution*] **promoting the development of an industry sponsored RegTech platform**, which could collect and disseminate (on a voluntary basis) RegTech solutions already implemented by EU financial institutions in a single website, provide information on functioning of reported solutions and help to connect financial institutions and RegTech providers in the EU. However, before proceeding, a comprehensive analysis should be conducted on how to address any arising competition issues to avoid promoting some solutions/technology providers in detriment of others;

2) [*medium term solution*] **certification of RegTech products, services and processes,** for example external ICT/cyber security certification for RegTech providers to demonstrate adherence to fundamental security principles and techniques of their technological solutions (potentially falling under the **EU cybersecurity certification framework**[32] that ENISA is currently working on). Such a certification would be only one component in the due diligence process;

3) [*long term solution*] **oversight of RegTech service providers,** that provide certain activities which pose risk or are relevant for financial stability. In particular, critical RegTech service providers might fall under an oversight framework, covering among others ICT and security, governance, operational and capacity aspects, in line with the 'oversight of third party providers' proposals presented in the European Commission's consultation document on Digital Operational Resilience Framework for financial services. This could create a culture of trust and facilitate to scale up solutions across the single market of EU.

Nevertheless, the costs and benefits of potential certification of RegTech services and/or registration of RegTech providers would need to be carefully assessed as such solutions will require ongoing monitoring of compliance with the related requirements while necessary measures should be taken to prevent unintended consequences on technological neutrality (e.g. of AML legislative acts) and to ensure proportionality. In addition, caution should be taken to prevent any perceived transfer of responsibility to third party service providers, which would be contrary certain regulatory requirements and to ensure a level playing field between critical RegTech providers and other critical third party providers (*e.g.* cloud service providers).

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:

The EBA highlights financial institutions' reporting regulations would benefit from the translation into machine-executable form. A clear benefit is the elimination of the need by institutions to interpret the legislation if not sufficiently clear, or the possibility of misinterpreting it otherwise. This would not only benefit the institutions, which could reduce their compliance and reporting

[32] https://www.enisa.europa.eu/topics/standards/certification

costs, but also the authorities, which would receive homogeneous data from the different institutions for their supervisory tasks, data expected to be also of higher quality. This more accurate and uniform industry reporting could also allow faster risk identification by regulators. This would also reduce the resources and time allocated to data validation, to the benefit of data analysis. Another advantage would be that changes in regulatory requirements could be implemented in a swifter manner. On the other hand, one of the main challenges of developing a proper machine-executable reporting regulation is that the underlying legislation, e.g. the CRR, may be too complex and difficult to automate. A way to overcome this would be to already translate into machine-readable form the underlying legislation, at least the parts directly related to calculations like the calculation of the capital requirements or the supervisory ratios. Converting those regulations may be in turn rather complex, in particular with the existence of national discretions and optionalities allowed by the regulations or possibly the different accounting standards. There may be a need to rethink the way regulations are conceived in order to be able to achieve the standardisation/ automation needed for a machine executable regulation. In doing so, it should be investigated whether these developments could bring any potential risk of reducing accountability and responsibility for financial reporting.

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:

From a reporting perspective, the EBA strongly supports the work on standardising concepts, definitions and reporting obligations across EU financial services legislation. Standardised concepts and definitions are necessary prerequisites for the digitalisation of supervision and the scale up of RegTech solutions, and especially in the area of supervisory reporting. Indeed, technological solutions are more likely to thrive where there are standardized protocols and structured data, on which technology-enabled applications can build and add value.

Together with standardisation, overall consistency should be ensured among different regulatory frameworks (e.g. the CRD/CRR package and the MiFID2/MiFIR framework) that may apply to the same intermediaries (e.g. credit institutions, investment firms). The ESAs can bring valuable views into this work and we stand ready to collaborate with the Commission on standardisation and harmonization of definitions and reporting obligations.

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? Please explain your reasoning and provide examples if needed:

The stronger use of supervisory data along with other publicly available data may increase the effectiveness of supervisory understanding through increased better knowledge of context. SupTech applications, in particular, are capable of combining multiple data sources (often

structured and unstructured data) to support analytical work. There are examples of successful use of combination of supervisory and other publicly available data, while consideration should be given to the scope and use of publicly available data for supervisory purposes.

For example, we have observed that:

(a) suspicious transactions reports (structured data) have been combined with press reviews (unstructured data) for AML/CFT purposes;

(b) social media data have been used to assess customers' sentiment towards specific companies and the effect on stock returns, volatility and trading volumes;

(c) news channels have been used to measure economic policy uncertainty and to investigate payment card scams;

(d) data from online real estate ads extracted from the web have been used to elucidate the structure of the real estate market in the relevant jurisdiction.

Potential benefits could be:

- **Enhanced effectiveness, reduced costs and improved capabilities,** assuming legacy IT systems have adequate capacity and do not pose a burden. The emergence of innovative technologies might significantly improve analytical capabilities while enhancing effectiveness. Potential cost reductions may result through data analytics solutions.
- **Improved traditional or manual processes and potentially faster supervisory action**. This may result from improved off-site monitoring, along with better and earlier detection of potential risks.
- **Enhanced supervisory capabilities through automating data gathering and analysis**, allowing the identification of potential supervisory issues. Moreover, the combination of available structured and unstructured data might enrich analyses. For example, considering that currently most of supervised institutions are using social networking websites to promote their products and services, social media data becomes really relevant to perform monitoring and supervisory activities, in particular to identify new products and services and to oversee the compliance with legal and regulatory requirements (e.g. advertising's oversight).

On the other hand, it should be taken into consideration that technical, data quality, legal, operational, reputational, resource, internal support and practical challenges may be encountered:

- technical issues relate to computational capacity constraints and lack of transparency on how some technologies work;
- data quality and completeness can be a concern for non-traditional sources of information (e.g. social media);

- enforceability of supervisory measures in case of reliance on (invalidated) publicly available media may be an issue;
- resource challenges in terms of having the right talent, skills and expertise;
- public data sources might include a lot of unstructured data, which can be difficult to handle;
- the reliance on social media data can cause privacy concerns.

The facilitation of the SupTech would require addressing the following issues:

- upgrading existing ICT infrastructure to enable collection and analysis of data;
- developing reliable technology-enabled supervisory solutions; and
- building the necessary skillsets and digital supervisory culture.

While the build-up of the necessary underlying IT infrastructure falls under the responsibility of individual competent authorities, it is important to ensure coordination to make sure that the systems remain compatible.

To increase the effectiveness of supervision via leveraging on technological innovation, an emphasis should be made in the medium-long term on the creation of the **European Strategy for the supervisory technologies (SupTech)**, recognising also the strong linkages between SupTech and RegTech, and leveraging on the experience from the existing SupTech solutions across competent authorities.

Additional funding could also be applied by the EBA to **facilitate the gathering of best practices and trends on SupTech and** promote/facilitate (collective) development of selected specific SupTech use cases for the benefit of supervisory and regulatory authorities in the EU. **The EBA could also act as a center for excellence and networking in this context and help instigate scalable SupTech across the Single Market.**

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

The EBA has highlighted in different publications the potential opportunities, risks and uncertainties that may come with the use of financial technologies, and sees technologies as an important enabler of sustainable development. At the same time some technologies can be resource intensive and some consideration to green labelling could be considered for key technologies.

For policy makers on digital transformation, it will be important to integrate environmental, social and governance (ESG) impact assessments as an integral part of policymaking, including digital transformation related policies. Such an assessment could guide policy makers in evaluating potential environmental impacts (and social impacts) of their policies. For instance, based on the EBA Regulation the EBA shall in its activities (including related to technological innovation) take into

account the integration of ESG related factors. Similar provisions are included in the mandates of other EU bodies. Having specific responsibility to conduct ESG impact assessments for all relevant public policy makers would support environmentally sustainable digital transformation.

Even though digitalisation offers new opportunities for European citizens, it is important to ensure that the integration of new technologies benefits society as a whole and does not exacerbate existing structural inequalities in society and/or market concentration in markets for financial products and services. In the context of climate-risks, the impact of both physical and transition risks is likely to be unevenly distributed affecting more severely low-income regions and households. It would be important to avoid that these impacts are amplified by that of digitalisation.

The EBA provides more details on a related question on how technologies can support sustainable development goals in its response to the consultation on the Renewed Sustainable Finance Strategy.