

Call for evidence

Digital Finance

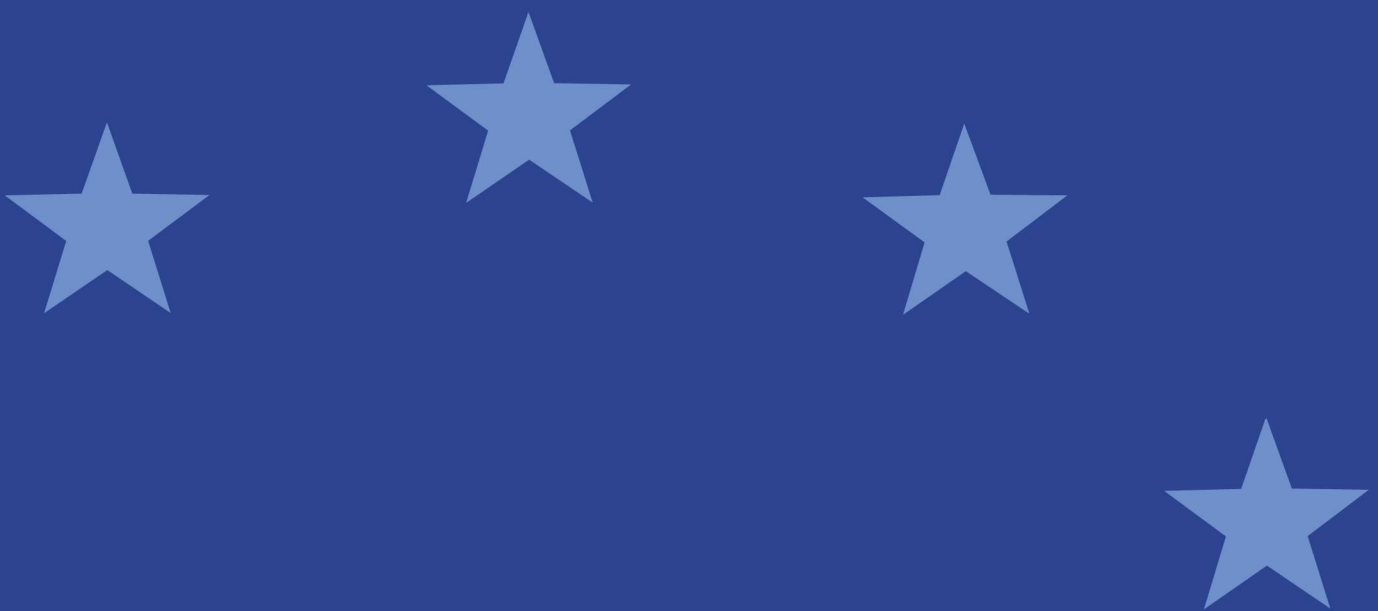


Table of Contents

1	Executive Summary	2
2	Introduction.....	3
3	More fragmented or non-integrated value chains.....	5
4	Platforms and bundling of various financial services	11
5	Risks of groups combining different activities	15

1 Executive Summary

Reasons for publication

Technological innovation is transforming financial services at an unprecedented speed, by facilitating new business models and services and the entrance of new market participants. Covid-19 is accelerating this shift and the digitalisation of financial services. These changes bring a host of opportunities, including the prospect of better financial services for businesses and consumers and greater financial inclusion. Yet, they raise challenges as well, as they can contribute to introduce or exacerbate new risks. Also, the existing regulatory and supervisory framework may not fully capture and address these new developments.

In September 2020, the European Commission (EC) published a digital finance package¹ with the aim to embrace digital finance in the EU. Following on the package, in February 2021, the EC set out a request for technical advice² to the European Supervisory Authorities (ESAs) on three main issues, namely (i) the growing fragmentation of value chains in finance, (ii) digital platforms and (iii) groups combining financial and non-financial activities. In particular, the ESAs are requested to assess the regulatory and supervisory challenges brought by these developments and the way in which they could be addressed. ESMA is seeking feedback from external stakeholders to inform its work on the matter.

Contents

Section 2 explains the background of this call for evidence. Sections 3, 4 and 5 set out the topics on which ESMA is asking for feedback and the questions. Appendix 1 summarises the questions.

Next Steps

ESMA will consider the information received through this call for evidence when drafting its response to the EC. ESMA, together with the other ESAs, need to deliver a report to the EC by 31 January 2022. The technical advice received from the ESAs will not prejudice the EC's decisions in any way.

¹ [Digital finance package | European Commission \(europa.eu\)](https://ec.europa.eu/press/press_corner/detail/2020/09/20200924-digital-finance-package)

² https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/210202-call-advice-esas-digital-finance_en.pdf

2 Introduction

1. *Digitalisation is transforming society, the economy and the financial sector. This transformation, and the application of innovative technologies in the EU financial sector, has the potential to benefit people and companies. By facilitating the entry of new market participants, reducing geographical barriers and promoting greater transparency in the provision of financial services, technological innovation can provide better financial services to a wider range of businesses and consumers, possibly at a lower cost. It can also foster financial inclusion.*
2. *Meanwhile, those changes are not exempt of challenges. The entry of - large and small - technology companies in financial services and the growing reliance on those companies by financial firms can give rise to new forms of risks, e.g., in relation to security, interconnectedness, concentration and competition.³ These changes raise specific regulatory and supervisory challenges as well, including due to their global and cross-sectoral nature and the risk of unlevel playing field.*
3. *The EC aims to address the challenges and risks attached to digital transformation by proposing, where relevant, adaptations to the existing legislative frameworks by mid-2022. To prepare these actions, and considering that regulation should be technology neutral according to the ‘same activity, same risk, same rule’ principle, the EC is requesting technical advice from the ESAs on the following key issues⁴:*
 - a. *more fragmented or non-integrated value chains arising as a result of the growing reliance by financial firms on third parties for the delivery of their services and the entry of technology companies in financial services;*
 - b. *platforms and bundling various financial services;*
 - c. *groups combining different activities, namely mixed activity groups providing both financial and non-financial services.*
4. *Importantly, the recent legislative proposals for the Digital Markets Act (DMA)⁵ – adopted on 15 December 2020 – and Digital Operational Resilience Regulation (DORA)⁶ intend to address some of the above risks and challenges already. DMA proposes new ex-ante rules for gatekeeper platforms as well as a new supervisory framework at EU level to address conduct and competition harm risks. Most of the large technology companies which are currently offering financial services are likely to fall into the scope of this proposal. Similarly, DORA proposes a new oversight framework for those ICT service providers that are critical to the financial sector, which is likely to apply to most of the large technology companies to the extent that they provide ICT services to financial firms. The framework aims to monitor and address concentration risk and systemic risk that may arise from critical third-party provision of ICT services. However, other gaps and issues, e.g., in relation to conduct or prudential risks or cooperation between relevant competent authorities, may be left unaddressed and require further adaptations to the existing regulatory and supervisory frameworks.*

³ For a detailed introduction on how BigTech firms are entering the financial services sector and the possible challenges and benefits associated with this development, please have a look at [ESMA’s ‘Trends, Risks and Vulnerabilities report 1/2020’](#).

⁴ The EC is also asking EBA for input in the areas of protection of client funds and non-bank lending.

⁵ https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

⁶ https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

5. *With this call for evidence (CfE) ESMA seeks the input of market participants, technology companies and other stakeholders on those remaining gaps and issues that would need to be addressed.*
6. *Noteworthy, ESMA is cooperating closely with EBA and EIOPA on these matters, leveraging on the work already undertaken, for example in the form of a survey on digital platforms to the industry⁷ for what concerns EBA or a Discussion Paper on the (re)insurance value chain and new business models arising from digitalization⁸ for what concerns EIOPA.*

General information about respondent

Name of the company / organisation	Association of Financial Markets in Europe (AFME)
Activity	Non-governmental Organisation and Other Associations
Are you representing an association?	<input checked="" type="checkbox"/>
Country/Region	Europe

Q1 Please insert here any general observations or comments that you would like to make on this call for evidence, including how relevant digital finance may be to your own activities.

AFME welcomes the Call for Evidence (CfE) and the efforts of the European Commission and ESMA to address the challenges and risks associated with the digital transformation of financial services. We believe the three trends identified by ESMA in the CfE are aligned with our observations. We observe technology companies entering financial services in three ways:

- As vendors (e.g., use of third party providers by financial entities),
- Partnering with incumbent financial service providers (e.g., partnering of third party providers with financial entities); and
- As standalone service providers (e.g., direct entry of technology providers in financial services).

While these changes are still under way and we cannot fully predict how they will ultimately unravel, we note that they represent both an opportunity and a potential source of disruption in financial services. We therefore welcome ESMA's efforts to consider how the EU policy frameworks may need to adapt to deal with emerging risks associated with these trends. In doing so, we encourage ESMA to consider two important dimensions:

- The impact on the level playing field, if regulatory approaches operate a differentiated approach between incumbent firms versus new entrants; and
- The potential risk of technology providers on financial stability if those providers remain outside the financial regulatory perimeter and continue to be subject to siloed, ad-hoc requirements when undertaking financial services activities.

In respect of the first trend (e.g., technology providers as vendors), and as emphasised in our responses below, financial entities are subject to existing regulatory requirements that govern their outsourcing relationships, including the EBA Outsourcing Guidelines and the ESMA Cloud Outsourcing Guidelines.

⁷ <https://www.eba.europa.eu/financial-innovation-and-fintech/fintech-knowledge-hub/regtech-industry-survey>

⁸ [EIOPA \(2020\). Discussion Paper on the \(re\)insurance value chain and new business models arising from digitalization.](#)

Furthermore, the proposed Digital Operational Resilience Act (DORA) will further tighten those obligations and introduce additional requirements. On this basis, we would caution against the development of new rules that look to govern how financial services firms engage third-party technology providers, particularly given that DORA is yet to be finalised, and that both outsourcing guidelines from the EBA and ESMA have only been recently finalised.

Regarding the second and third trends, we acknowledge the need to ensure that any risks stemming from the entry of technology providers into the financial services sector are appropriately addressed. For example, while it is proposed that critical ICT third party providers will be brought into the scope of an oversight framework under DORA, they will remain governed indirectly by obligations imposed on incumbent financial entities and will not be subject to direct requirements on risk management, resilience and governance. As a starting point the principle of 'same activity, same risk, same regulation' should be adhered to on a proportionate basis, while assessing potential adjustments required, should risks not be sufficiently mitigated.

As mentioned, we believe that the current focus of this CfE is an accurate reflection of the current state of digital finance and potential issues this may create. We believe a more forward-looking approach should also be considered regarding the long term potential of technology innovation and opportunities this may bring to financial services (e.g., growth, innovation, creation of fintech ecosystems, enhanced capabilities).

3 More fragmented or non-integrated value chains

7. *Technological developments are increasing the extent to and ways by which financial firms rely on third-parties, in particular technology firms, for the delivery of services, thereby leading to more fragmented or non-integrated value chains. This dependency can take different forms, e.g., outsourcing, partnerships, cooperation agreements or joint ventures. Examples include cloud outsourcing arrangements or the use of technology companies for data analytics, risk management or marketing purposes. In addition, digital innovation facilitates the entry of technology companies in financial services, again leading to potentially closer interlinks and increased inter-dependency between those companies and financial firms.*
8. *These new business models may entail various benefits, such as increased efficiency. However, they may also introduce new risks and may not be fully captured by the existing regulatory framework. Indeed, the entities contributing to the provision of the financial services may be subject to a set of individual requirements in the absence of a holistic approach or even fall outside of the regulated space. These models may also raise challenges in relation to cross-border supervision, cooperation between different competent authorities, as well as legal responsibility for conduct, operational resilience of the entire value chain and prudential treatment.*
9. *This call for evidence aims to collect evidence on new material developments in the evolution and fragmentation of value chains and the extent to which this phenomenon introduces new risks and/or create regulatory and supervisory challenges.*

Questions

- Q2 Do you observe changes in value chains for financial services (e.g., more fragmented value chains) as a result of technological innovation or the entry of technology firms? How different is the situation now when compared to pre-Covid?**

AFME acknowledges that technological innovation and the entry of technology firms is increasing within financial markets (e.g., the use of cloud services and providers, increased adoption of artificial intelligence, innovation in distributed ledger technology and digital assets). This trend has continued during the COVID19 pandemic and has contributed to an increased role of technology providers within financial markets value chains.

In November 2020, AFME published a report with PwC analysing trends in technology and innovation in Europe's Capital Markets⁹. The report highlighted the importance of technology providers supporting innovation within financial markets.

Outside of capital markets, we note that technology providers are increasingly involved in other areas of financial services such as payments (e.g., data processors and aggregators), the distribution of financial products and services on digital platforms or in the development of application programming interfaces (APIs). This can pose challenges and risks for financial services value-chains. For example, in some cases, payments services by technology providers to merchants is an unregulated technical service. Further, the development of APIs may enable the distribution of financial products and services on digital platforms or digital marketplaces, which makes it more difficult for customers to identify the responsible party and underlying risks.

We acknowledge that recent policy developments on outsourcing and operational resilience are looking to address these risks more extensively. However, we note that whilst DORA, for example, may bring critical third party providers into the scope of an oversight regime, DORA introduces additional risk management requirements only for financial entities. We believe technology providers involved in the conduct of financial services activities should be held to similar standards of governance, risk management and resilience as financial institutions. We believe it is essential that technology providers do not negatively impact financial stability, digital operational resilience, security, and data protection and privacy.

We note that some financial services value chain changes have been driven by regulation (e.g., PSD2, which has opened the market for payment service providers in retail banking). We believe regulatory initiatives aiming to increase access and competition should also consider impacts on investor protection (e.g., the ability to clearly identify service providers and underlying risks), AML/CTF (e.g., the involvement of third parties operating with weaker standards than incumbent financial firms), operational risks (e.g., to the risk of potential third-party failures) and financial stability (e.g., where non-regulated entities are interacting with clients).

We also note ongoing policy developments such as the Digital Market Act (DMA), currently under negotiation, which aims to address competition issues related to technology providers and digital platforms.

Q3 Do you consider that financial firms are increasingly relying on technology firms to fulfil critical or important functions? If so, for which particular functions? Are there particular types of technologies (e.g., BigData, artificial intelligence, cloud computing, others) and technology firms involved?

AFME believes that the reliance on technology providers by financial firms to fulfil critical or important functions remains limited. Regarding particular technologies being adopted, our November 2020 report with PwC highlighted four main focus areas; cloud, data and analytics, artificial intelligence and distributed ledger technology.

⁹ https://www.afme.eu/Portals/0/AFME_TechnologyInnovation_FINAL.pdf?ver=2020-11-13-135131-297

However, regardless of the role of technology companies, financial firms remain responsible for the resilience and provision of their critical or important functions. As such, financial entities must comply with multiple regulatory requirements (e.g., resolution planning, outsourcing and resilience requirements) to ensure the safe, secure, and resilient provision of critical or important functions. In addition, financial firms have extensive security and technology controls.

The use of technologies, such as cloud computing, are increasingly being used to support some critical or important functions within financial firms (e.g., core banking environments). This involves technology firms being providers of some elements of critical or important functions through outsourcing. Further, the use of artificial intelligence and Big Data may increasingly be used by financial entities (e.g., corporate control or KYC-related processes), which could include some elements of critical or important functions.

For instance, financial entities increasingly use technology providers (e.g., fintechs, partnership with existing infrastructures) for capital markets post-trade services to fulfil a variety of functions, including: document digitization, workflow, exception management, blockchain SaaS, market data providers, analytics, and data storage for both digital and traditional assets. Often, new technology provider offerings are provided across product and/or lifecycle services (e.g., allocation, confirmation, settlement, asset servicing), rather than specializing in one key function like their predecessors. This creates an opportunity for less fragmentation in the future.

The use of technology providers often allows financial entities to achieve levels of security and resilience which they could not reach with in-house IT infrastructure. For example, cloud computing allows the ability to failover across multiple availability zones or regions and roll out security patches more consistently and quickly. We acknowledge there remain risks in using third-party technology providers. However, these are being addressed through industry best practices and regulatory requirements, both of which have received significant attention in recent years. Therefore, we believe that additional time is required to assess regulatory and industry practices before any further action is considered by EU authorities.

Q4 Do you have examples of technology companies providing financial services in the EU, either directly or through arrangements with financial firms? If so, please briefly describe their business model and the type of financial services that they provide.

AFME is not aware of technology companies providing financial services in capital markets directly to clients in the EU. However, we note that technology companies are increasingly providing financial services related to crypto-asset trading, which will likely be addressed by the Commission's proposed MiCA regime. We also observe technology companies providing services related to payments, data aggregation, and lending.

Therefore, we believe it is appropriate for ESMA to continue to monitor technology companies providing financial services in the EU. For example, the rapid expansion of payment service providers within retail financial markets and future considerations this may bring to capital markets could be a first area of focus. We are aware that this trend is taking place in other jurisdictions, as observed in the 2019 BIS report 'Big tech in finance: opportunities and risks'¹⁰. In certain jurisdictions, the incursion of technology companies into financial services has been extremely rapid, noting differences compared to the EU in terms of applicable regulation.

¹⁰ <https://www.bis.org/publ/arpdf/ar2019e3.pdf>

Q5 Do you have examples of technology companies being used by financial institutions in the EU to fulfil critical or important functions? If so, please briefly describe their business model and the way in which they contribute to, or facilitate, these critical or important functions.

AFME has not responded to this question.

Q6 Do you see changes in the way or extent to which financial market data are being collected, used and disseminated by unregulated data service providers?

We observe trends towards vertical integration through:

- Services providers of financial market data generating data or data analysis (e.g., offering additional services based on raw market data), and;
- Services providers being acquired by companies within the value chain which may impact on the unrestricted access to data from other data distributors.

Technological innovation and new market entrants could bring distinct risks and benefits to market data reporting. For example, using new technologies such as Artificial Intelligence (AI) to improve data collection and reporting efficiency (e.g. using natural language programming to interpret large volumes of structured and unstructured market data).

At the principle level, if there is a need to mitigate potential risks, this should not be done at the cost of suppressing the benefits that can be derived from technical innovation. Therefore, before any policy decisions are made, a full cost/benefit analysis with all industry stakeholders must take place to fully understand the benefits and risks of technological innovations within market data. This will ensure that the regulatory framework remains technology-neutral and supportive of innovation.

For further detail on AFME's position on market data guidelines, please see our response on this topic ([here](#)).

Q7 What implications, if any, do changes in value chains (e.g., more fragmented value chains) have on your own activities? To which extent are you taking an active role in these changes?

We note that recent ESMA and EBA Guidelines on cloud and outsourcing set out requirements for financial firms which govern the controls around cloud, supply chain, and sub-outsourcing. These Guidelines have implications on financial firm activity as they govern how supply chain risk should be addressed.

The trend of subcontracting is contributing to more fragmented value chains and may present certain risks. In the context of data sharing, for example, where there is a 4th party involved, firms may not have confidence that standards on data protection or cyber security are being applied consistently, which may hamper data sharing. This further reinforces the need to ensure the application of common minimum standards across the value chain and not just on financial institutions.

Regarding the role of technology providers increasingly supporting innovation, please see our response to Question 2.

Q8 Do you see new or exacerbated risks (e.g., to investor protection, financial stability, market integrity, security or level playing field) in relation to the reliance on technology firms by financial firms?

Where technology providers are directly or indirectly involved in providing critical functions supporting financial services, AFME believes it is essential that these service providers adhere to a similar level of digital operational resilience as regulated financial entities. Digital operational resilience standards should be developed with proportionality in mind so that all relevant financial market participants adhere to appropriate standards. For instance, we note that DORA aims to introduce additional obligations on financial entities for risk management, resilience, and business continuity. DORA also aims to introduce an oversight regime for ICT Critical Third Party Providers (ICT CTTPs), which would allow competent authorities to have more visibility into these providers, but would not elevate them to the same level of standards as financial institutions. We therefore urge regulators to exert caution when considering additional requirements applicable to financial entities, given the number of recent regulatory guidelines and requirements on outsourcing, third party risk and ICT risk management. However, we also note that NISD2 and DORA could present benefits and efficiencies for EU financial services by increasing assurances for third party use by financial firms.

In this context, we acknowledge the recent publication by the Financial Stability Institute (FSI) on the applicability of a level playing field for Fintech regulation. In particular, the report notes that risks related to BigTech activity in finance may not be fully captured by current regulatory approaches (e.g., geared towards individual entities or specific activities). This is because BigTech firms leverage innovative business models, are able to scale up quickly, and may become systemic in nature.

From an antitrust standpoint, it will be important that any developments seeking to bring third parties with the regulatory perimeter, such as DORA, do not lead to the inadvertent disclosure of commercially sensitive information between competing firms.

Q9 Do you see new or exacerbated risks (e.g., to investor protection, financial stability, market integrity, security or level playing field) in relation to the provision of financial services by technology companies?

From a competition perspective, AFME believes it is generally positive that the number of providers offering a specific service increases. However, any new entrants should have the required expertise to offer adequate guarantees of safety and reliability for clients. The financial sector is already highly regulated in this regard compared to new entrants, who may well have to comply with certain obligations based on the activities they perform but are not supervised holistically in terms of their risk management and governance processes.

We support a regulatory framework that is technology-neutral and supportive of innovation, which applies the principle of 'same risk, same activity, same regulation' and is consistent with global standards. However, it will be important for regulators to consider what technology providers may fall under the regulatory perimeter if they take a more critical role or directly engage with clients (e.g., providing services akin to a regulated financial firm). We believe any changes identified to the regulatory perimeter should be considered globally and consistently applied across the EU.

Q10 Do you see new or exacerbated risks (e.g., to investor protection, financial stability, market integrity, security or level playing field) in relation to the collection, use and dissemination of financial market data by unregulated data service providers?

For further detail please see our response to question 6 and 8.

Q11 Do you consider that some adaptations to the EU regulatory framework are needed to address the risks brought by changes in value chains?

We note that the financial sector is currently undergoing significant review and changes in terms of applicable requirements for outsourcing, third party risk management and ICT risk management (e.g., EBA and ESMA Outsourcing GLs, EBA ICT GLs, DORA, BCBS Operational Resilience Principles, FSB Outsourcing). We believe greater scrutiny of existing regulatory asymmetries, as identified by the FSI¹¹, need to be conducted to identify how these may be contributing to level playing field issues as well as a build-up of risks to financial stability.

As referenced in response to Question 1, regarding the direct entry of technology companies into financial services, we acknowledge the need to ensure that any risks are appropriately addressed and that the principle of 'same activity, same risk, same regulation' is adhered to on a proportionate basis.

Regarding the use of third third-party providers by incumbent financial services firms, we support existing outsourcing guidelines developed by both ESMA and the EBA. We also acknowledge the potential benefits of the European Commission's proposal on the Digital Operational Resilience Act (DORA), where AFME is developing recommendations to support the ongoing negotiations. This policy initiative will be relevant in situations where financial entities are using third party providers. On this basis, we would therefore caution against the development of new rules that look to govern how financial services firms engage third-party technology providers, particularly given that DORA is yet to be finalised, and that both outsourcing guidelines from the EBA and ESMA have only been recently finalised.

Regarding the regulation of technology providers themselves, AFME notes that DORA will play an important role in bringing ICT Critical Third Party Providers (CTPPs), including Cloud Service Providers (CSPs), under a framework for direct oversight. This should improve visibility into ICT CTPPs but will not directly impose requirements to promote investor protection, financial stability, market integrity and security objectives on ICT TPPs.

From an antitrust standpoint, relevant laws and regulations allow competent antitrust authorities (EU and national) to intervene when the conduct of financial firms – including new entrants – may cause a restriction, distortion, or elimination of competition in financial markets (irrespective of the nature of the firms involved and the business sector they operate). However, in certain circumstances, some adjustments may be required. As stated in our response to question 2, we note ongoing policy developments such as the DMA, currently under negotiation, which aims to address fair competition shortcomings due to technology providers, such as digital platforms.

Please see our response to question 2 regarding value chain changes observed in financial services and have been driven by regulation.

Please see our response to Question 9 regarding considerations of what entities may fall under the regulatory perimeter.

Q12 Do you consider that some adaptations to the EU regulatory framework are needed to unlock the benefits brought by changes in value chains?

Please see our response to question 2.

¹¹ <https://www.bis.org/speeches/sp210616.htm>

Q13 Do you consider that there is a need to enhance supervisory practices, e.g., cross-border or cross-sectoral cooperation, in relation to changes in value chains?

AFME fully supports enhanced cross-border and cross-sectoral cooperation.

Given the ability of technology providers to operate on a cross-sectorial and cross-border basis, any regulatory response that looks to supervise those providers directly should be appropriately coordinated to prevent the development of siloed and duplicative regulatory frameworks.

As a starting point, the principle of 'same activity, same risk, same regulation' should be adhered to on a proportionate basis while assessing potential adjustment required, should risks not be sufficiently mitigated.

However, possible adaptations to existing regulatory and supervisory frameworks should be considered where technology companies providing financial services are regulated differently to incumbents' under the existing regulatory framework. This is the case, for example, where a new market entrant has entities within their group providing financial services, but the group itself does not fall within a consolidated application of the prudential framework.

We also support regulatory and supervisory upskilling to better understand and ascertain the impact of technology transformation on financial services.

Finally, any changes to the regulatory perimeter should be considered in a global context for cross-border financial firms and consistently applied across the EU to support the adoption of new technologies and business models.

Q14 Which recommendations, if any, would you make to EU regulators/supervisors to address opportunities and challenges brought by changes in value chains?

For further detail please see our response to question 2.

Q15 Do you have any other observations or comments in relation to changes in value chains?

AFME has not responded to this question.

4 Platforms and bundling of various financial services

10. Platforms can market and provide access to multiple different financial services, often from different financial firms. Different financial firms can also partner with technology firms to bundle a range of financial services which are then distributed through digital channels.

11. The financial firms and platform providers are not always part of the same group and sometimes operate in different EU Member States or third countries. In addition, the different financial services bundled on the platform may fall under separate sectorial regulations or outside of the scope of the EU financial services regulatory perimeter, which can leave certain risks unaddressed and raise specific supervisory challenges.

12. A more holistic approach to the regulation and supervision of these platforms and bundled services could be relevant, considering the increased risk that they can pose, regarding e.g. interaction with consumers and consumer protection, conduct of business, money laundering and operational risk.

13. The CfE is intended to help ESMA collect insights on the use of digital platforms in the EU the extent to which this phenomenon introduces new risks and/or create regulatory and supervisory challenges.

Questions

Q16 Do you have examples of platforms bundling different financial services from different financial firms in the EU? If so, please provide a brief description of the most prominent ones.

We are not aware of platforms bundling different financial services from different financial firms within EU capital markets.

This bundling may be more prevalent in other jurisdictions or financial market sectors within financial services (e.g., retail banking, insurance) as stated in the 2019 BIS report 'Big tech in finance: opportunities and risks'¹². For example, we noted the existence of online trading platforms which offer products ranging from FX, equity, cryptocurrency, ETFs, investment funds and commodity brokers.

We note that in retail banking, such as mobile banking, some examples may include:

- Mobile wallets (e.g., to access payment services from multiple providers), and;
- Financial market places (e.g., to access new saving options).

We note that the existence of platforms within financial services has grown rapidly in certain jurisdictions (e.g., China), leading to the emergence of new financial stability risks for regulators. Whilst the EU may be in nascent stages in terms of the prevalence of platforms bundling different financial services, we note this could change rapidly.

Q17 Do you consider that the use of platforms by financial firms for the marketing or the conclusion with customers of financial products and services is widespread in the EU? Do you observe an increase in the use of platforms compared to pre-Covid?

We do not currently believe there is widespread use of platforms by financial firms for the marketing or the conclusion with customers of financial products and services within EU capital markets. We note some platform developments within trade finance.

However, we note an increased interest of some private clients to use online sales platforms for competitive comparison and digital purchases of retail products and a general increase in EU business via platforms. While these trends existed pre-Covid, they may have accelerated due to remote working and increased access to digitally recorded information (e.g., products, confirmations, valuations).

¹² <https://www.bis.org/publ/arpdf/ar2019e3.pdf>

Q18 (To financial firms) As a financial firm, are you using platforms for the marketing or the conclusion with customers of your financial products and services? If yes, please provide a brief description of(i) the types of services provided by the platform, (ii) the arrangement in place with the platform (e.g., are you or the platform responsible for the governance and/or maintenance of the technical infrastructure and the interactions with customers), (iii) the extent and way in which the arrangement is disclosed to the customer, (iv) the tools and processes in place to ensure that the risks attached to the financial products and services are properly disclosed to the customers.

Arrangements vary depending on the third party provider, but broadly technology companies are responsible for maintenance of the technical infrastructure, and financial entities retain responsibility for interactions with customers; governance may be shared (e.g., Joint Venture, partnership, etc.).

Q19 (Same question to platforms) As a platform, do you facilitate the marketing or the conclusion with customers of financial products and services? If yes, please provide a brief description of(i) the types of services provided to financial firms, (ii) the arrangement in place with the financial firms (e.g., are you or the financial firm responsible for the governance and/or maintenance of the technical infrastructure and interactions with customers), (iii) the extent and way in which the arrangement is disclosed to the customer, (iv) the tools and processes in place to ensure that the risks attached to the financial products and services are properly disclosed to the customers.

AFME has not responded to this question.

Q20 Which key opportunities and challenges do you see in relation to the use of platforms by financial firms?

AFME agrees with ESMA's general statement that digital platforms may offer benefits to financial firms by marketing and enabling clients to access multiple financial services (often from different financial entities). Financial firms may also use digital platforms, managed by technology firms, to access and distribute their products and services through digital channels to reach a broader range of potential clients and integrate financial services into other value propositions. However, AFME has not observed increased digital platforms (e.g., bundling of services) within EU capital markets.

Opportunities could include increased automation, straight-through-processing (STP), industry standardization and lower operating costs. However, this will require significant investment by financial firms to develop digital value-chains that can leverage multiple platforms (e.g., IT development and connectivity). It will also be essential that compliance with regulatory requirements is ensured for both financial firms and digital platform companies.

An important feature of digital platforms is the market interconnection they can bring (e.g., a network effect), as the monetisation of a service could occur in a different market than the one in which the service is offered. When applied to financial services, this could have various consequences, for instance, the risk of monopolistic or dominant market positions, financial stability risks (linked to zero-price dynamics), bank disintermediation, or consumer protection.

Based on these considerations, digital platforms may warrant careful attention by financial services regulatory and supervisory authorities, beyond the developments envisaged within the DMA, to ensure any risks to consumers, fair market practices, or financial stability are addressed effectively and proportionately. We encourage increased cooperation between regulatory authorities to understand the challenges posed by digital platforms. Initiatives such as the BIS Innovation hub and the European Forum for Innovation Facilitators (EFIF) should be encouraged.

Q21 Do you consider any of the following risks to be new/exacerbated where financial firms use platforms for the marketing or conclusion with customers of contracts for financial products and services? Please explain(i) risk to financial stability, (ii) risk to investor protection, (iii) risks in relation to conduct of business, (iv) ICT and security risks, (v) money laundering / terrorism financing, (vi) risk to data protection and privacy, (vii) risk to fair competition, (viii) market manipulation, or (ix) other risks.

Digital platforms may warrant careful attention by regulatory and supervisory authorities to ensure any risks to consumers, fair market practices, or financial stability are addressed effectively and proportionately.

With regards to data protection and privacy, we believe that digital platforms should not exacerbate risks as long as GDPR provisions are respected (e.g., data subject consent for marketing activities, Data Protection Impact Assessments in cases of AI driven advisory/profiling activities, valid data transfer tools in case of transfer of personal data outside EEA). However, we note that if responsibilities are not clearly delineated, this could lead to more complexity when identifying a liable party.

From an antitrust standpoint, it will be important that interactions with third parties are managed carefully to avoid disclosing commercially sensitive information between competing firms.

We encourage increased cooperation between regulatory authorities to understand the challenges posed by digital platforms. Initiatives such as the BIS Innovation hub and the EFIF should be encouraged.

Q22 (For financial firms) Which controls, and processes are in place to oversee the specific risks emerging from the use of platforms?

Regulated financial institutions have extensive controls and processes in line with regulatory requirements to oversee risks arising from their activities. Regulatory policy spanning outsourcing, data protection, AML/fraud, third party risk management and use of emerging technology, all translate into detailed internal policies for firms and how they approach the potential use of platforms.

Q23 Do you consider that some adaptations to the EU regulatory framework are needed to address the risks brought by the use of platforms?

For further detail please see our response to question 13.

Q24 Do you consider that some adaptations to the EU regulatory framework are needed to unlock the benefits brought by the use of platforms?

Considerations for transparency and a level playing field (e.g., consistent regulatory treatment for financial services related activities) will be important to ensure that the benefits of the use of platforms can be achieved (e.g., platform fee structures).

For further detail please see our response to question 22.

Q25 Does the use of platforms give rise to any challenges regarding the cross-border supervision of financial sector activities in the EU? Do you consider that there is a need to enhance supervisory practices, including convergence measures, in relation to the use of platforms?

AFME fully supports enhanced cross-sectoral and cross-border cooperative arrangements.

We believe the regulatory framework should remain technology-neutral, supportive of innovation, consistent with global standards, and applied in the principle of 'same risk, same activity, same regulation'.

It will be important for regulators to consider what entities may fall under the regulatory perimeter, should some entities take a more critical role or directly engage with clients and begin to provide services akin to a regulated financial entity.

Any changes to the regulatory perimeter should be considered in a global context for cross-border firms and consistently applied across the EU to support the adoption of new technologies and business models.

A thorough analysis of activity-based versus entity-based regulation should be performed by ESMA, in collaboration with the EBA.

Regarding antitrust, see our comment under Question 11.

Regarding level playing field, see our comment under Question 24.

Q26 Which recommendations, if any, would you make to regulators/supervisors to address opportunities and challenges brought by the use of platforms?

From an antitrust standpoint, see our comment under Question 11.

Regarding level playing field, see our comment under Question 24.

5 Risks of groups combining different activities

14. Large technology companies active in various sectors and forming mixed-activity groups increasingly enter the financial services sector, including through the establishment of their own subsidiaries for the provision of financial services. These groups can quickly scale up the offerings in financial services leveraging on vast amounts of customers' data collected through their affiliated entities and elevating intra-group dependencies on operating systems and processes. The capacity to use intra-group data and other processes within the group to support the provision of financial services raises challenges in relation to conduct, prudential and systemic risks and a possible detrimental effect to the level playing field between entities providing the same financial services as a part of a group versus a single entity.

15. Even though existing sectoral financial legislation already embeds approaches for group supervision, it does not provide a framework for coordinated supervision on a cross-sectoral basis for emerging types of mixed activity groups, as their financial activities usually represent only a

limited share of their total balance sheet. Even when a group has a specialised financial subsidiary undertaking within its group, sectoral financial legislation would only apply to that subsidiary undertaking, with limited possibilities to supervise and prevent risks stemming from the interactions between the financial subsidiaries and the broader group.

16. *The new emerging risks in relation to mixed-activity groups that build up substantial market share in financial services may not be captured by the existing EU legislation and by supervisory practices limited to regulated entities in the mixed-activity groups.*

17. *The call for evidence aims to collect evidence on whether (i) large technology companies as mixed-activity groups should be supervised specifically, (ii) how interdependencies within the groups, and potential risks stemming from, can be identified and addressed, and (iii) how supervisory cooperation can be improved for these groups.*

Questions

Q27 Are you aware of mixed activity groups (MAGs), including BigTech groups, whose core business is not financial services but that have subsidiary undertakings that provide financial services in the EU?

We are not aware of mixed activity groups (MAGs), including BigTech groups, whose core business is not financial services but have subsidiary undertakings that provide wholesale financial services within EU financial markets. However, this may be more prevalent in other jurisdictions or financial markets sectors (e.g., retail banking, retail payments, insurance) as stated in the 2019 BIS report 'Big tech in finance: opportunities and risks'¹³.

However, we agree that there is a need to ensure a continued focus on the entry of technology providers in financial services. To the extent that technology providers can leverage data to influence the provision of financial services, this can potentially enable the rapid scaling of financial services subsidiaries. This highlights the importance of ensuring that, to the extent that technology providers were to enter capital markets, the principle of 'same activity, same risk, same regulation' is adhered to for managing any consequential conduct, prudential, and systemic risks.

While we have yet to identify the direct entrance of BigTech companies' into EU wholesale markets, this situation could evolve in the future. We welcome the continued monitoring and dialogue with financial services authorities so that an appropriate policy response is implemented in such a situation.

Please also see our comments on BigTech providers in our response to the European Commission Consultation Paper on 'A New Digital Finance Strategy for Europe / Fintech Action Plan'¹⁴.

Q28 Which types of financial services do these entities provide?

AFME has not responded to this question.

Q29 In such MAGs, how and to what extent the dependency of a subsidiary financial firm on its parent company and/or other subsidiaries of the same group influences the provision of the financial service?

¹³ <https://www.bis.org/publ/arpdf/ar2019e3.pdf>

¹⁴ [https://www.afme.eu/Portals/0/DispatchFeaturedImages/20200626%20AFME%20EC%20CP%20Digital%20Finance%20\(FINAL\).pdf](https://www.afme.eu/Portals/0/DispatchFeaturedImages/20200626%20AFME%20EC%20CP%20Digital%20Finance%20(FINAL).pdf)

We note there may be important differences between MAGs which have a subsidiary offering financial services, and a financial entity, from a regulatory compliance and risk management perspective.

In particular, in the case of MAGs, financial services are offered as an ancillary service. This could mean that financial services are offered within the MAG not only to generate revenue but also to complement other service offering or generate clients insights through the use of data. This could lead to innovative business models supported by complex inter-group arrangements (e.g., integrated data pools, IT systems, common processes) with other non-financial businesses, within the MAG.

We are supportive of the ESAs role to assess risks related to groups combining different activities and how those potential risks could be mitigated through consolidated supervision or other means, with proportionality in mind. Assessing risks stemming from MAGs may require the cooperation and collaboration of multiple relevant authorities, given the ability of technology providers to operate on a cross-sectorial and cross-border basis. Any regulatory response that looks to supervise those providers directly should be appropriately coordinated to prevent the development of siloed and duplicative regulatory frameworks.

Q30 Do you see new or exacerbated risks in relation to MAGs?

As a starting point, the principle of 'same activity, same risk, same regulation' should be adhered to on a proportionate basis while assessing potential adjustments required, should risks not be sufficiently mitigated. Given the scale and systemic nature of some technology providers, considerations beyond the principle of 'same activity, same risk, same regulation' may be required to mitigate the systemic risk these providers could present. Any changes identified to the regulatory perimeter should be principles based, proportionate to risks, considered in a global context, and consistently applied.

We are supportive of the ESAs role to analyse and appropriately assess risks related to groups combining different activities and how those potential risks could be mitigated through consolidated supervision or other means, with proportionality in mind. Assessing risks stemming from MAGs may require the cooperation and collaboration of multiple relevant authorities, given the ability of technology providers to operate on a cross-sectorial and cross-border basis. Any regulatory response that looks to supervise those providers directly should be appropriately coordinated to prevent the development of siloed and duplicative regulatory frameworks.

Q31 Do you consider that there is a risk of unlevel playing field between individual ('solo') financial firms and MAGs?

AFME believes there could be a risk to the level playing field between individual financial firms and MAGs if the principle of 'same activity, same risk, same regulation' is not applied appropriately.

This is because of the consolidated application of prudential requirements for regulated financial firms, which applies to all entities within the banking group, irrespective of the activity and the risks involved for financial stability. As a result, when financial firms perform non-core activities (i.e. not funded with deposits), such as developing innovative technologies, they could have a higher cost/time-to-market than technology providers, subject to activity-specific regulation. As a result, regulated financial entities competing for innovative technologies with non-regulated entities could be treated differently. This entity-based approach to regulation could limit banks' ability to adapt their business and innovate, compared to non-banks performing similar activities that only need to apply bank-level controls to their banking subsidiaries. We support an assessment of how the principle of 'same activity, same risk, same regulation' could apply to non-financial services firms which have entities within their group that provide financial services.

We acknowledge the recent publications by the Financial Stability Institute (FSI) on the applicability of a level playing field for Fintech regulation. The report identifies:

- Risks related to BigTech activity in finance may not be fully captured by current regulatory approaches (e.g., geared towards individual entities or specific activities);
- Oversight of BigTech activity in finance may require a mix of entity-based and activity-based rules; and
- A need to enhance cross-sectoral and cross-border cooperative arrangements.

Also, we believe that differences in regulatory treatment between BigTech and traditional financial entities, in those areas where firms are conducting similar activities but are not regulated the same way, could put financial entities at a disadvantage. For instance:

- Remuneration limits; and
- Regulatory requirements (e.g., such as the consolidated application of prudential requirements applicable to all entities within the banking group).

As previously stated, given the scale and systemic nature of some technology providers we support an assessment of how the principle of 'same activity, same risk, same regulation' could apply to non-financial services firms which have entities within their group that provide financial services. Alongside the consistent application of regulatory requirements, we also believe in the consistent application of supervision. We believe technology providers involved in financial services activities should be held to similar standards of governance, risk management and resilience as financial institutions.

We also believe that for any future assessment of PSD2, regulators should ensure that further requirements for the sharing of financial firms data to third parties should be reciprocal and promote a level-playing field whilst ensuring privacy and security of data. This will ensure that financial firms continue to invest in innovation for the benefit of clients and the market whilst maintaining the resilience of their technology infrastructure.

Q32 In your opinion, is the current EU regulatory framework adequate for MAGs?

Please refer to our response to Question 30.

Q33 Do you consider there is a need for new cooperation and coordination arrangements between financial supervisors and other authorities (data, competition, consumer protection, AML/CFT, cyber) within the EU and/or with 3rd countries in order to ensure effective supervision of MAGs?

AFME fully supports enhanced cross-sectoral and cross-border cooperative arrangements.

We believe the regulatory framework should remain technology-neutral, supportive of innovation, consistent with global standards, and applied in the principle of 'same risk, same activity, same regulation'. However, given the scale and systemic nature of some technology providers, we acknowledge that further considerations beyond the principle of 'same activity, same risk, same regulation' may be required to mitigate the systemic risk they could present. Also, given the complex nature of MAGs (e.g., ability to operate on a cross-sectoral and cross-border basis), it may be challenging for a single firm or authority to effectively assess or mitigate risks stemming from MAGs. We believe this could require the collaboration of multiple authorities and jurisdictions to effectively identify and assess MAG related risks. AFME welcomes that the industry is further engaged on this topic.



However, we believe that any changes identified to the regulatory perimeter should be considered globally and consistently applied across the EU.

Regarding data protection, to the extent technology providers provide financial services in the EU and are subject to the GDPR, we consider the need for cooperation and coordination between authorities.

From an antitrust standpoint, see our comment under Question 11.