BANKING AND FINANCE

# Public consultation on FinTech: a more competitive and innovative European financial sector

Fields marked with * are mandatory.

## Introduction

Thank you for taking the time to respond to this consultation on technology-enabled innovation in financial services (FinTech). Our goal is to create an enabling environment where innovative financial service solutions take off at a brisk pace all over the EU, while ensuring financial stability, financial integrity and safety for consumers, firms and investors alike.

---

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

More information:

- on this consultation
- on the protection of personal data regime for this consultation

## 1. Information about you

*Are you replying as:

- ◯ a private individual
- ◉ an organisation or a company
- ◯ a public authority or an international organisation

*Name of your organisation:

American Chamber of Commerce to the European Union

Contact email address:

**The information you provide here is for administrative purposes only and will not be published**

stefano.marmo@amchameu.eu

*Is your organisation included in the Transparency Register?

(If your organisation is not registered, we invite you to register here, although it is not compulsory to be registered to reply to this consultation. Why a transparency register?)

- ◉ Yes
- ◯ No

*If so, please indicate your Register ID number:

5265780509-97

*Type of organisation:

- ◯ Academic institution
- ◯ Consultancy, law firm
- ◉ Industry association
- ◯ Non-governmental organisation
- ◯ Trade union
- ◯ Company, SME, micro-enterprise, sole trader
- ◯ Consumer organisation
- ◯ Media
- ◯ Think tank
- ◯ Other

*Please indicate the size of your organisation:

- ◯ less than 10 employees
- ◉ 10 to 50 employees
- ◯ 50 to 500 employees
- ◯ 500 to 5000 employees
- ◯ more than 5000 employees

*Where are you based and/or where do you carry out your activity?

Belgium

*Field of activity or sector (*if applicable*):

*at least 1 choice(s)*

- [ ] Accounting
- [ ] Asset management
- [ ] Auditing
- [ ] Banking
- [ ] Brokerage
- [ ] Credit rating agency
- [ ] Crowdfunding
- [ ] Financial market infrastructure (e.g. CCP, CSD, stock exchange)
- [ ] Insurance
- [ ] Investment advice
- [ ] Payment service
- [ ] Pension provision
- [ ] Regulator
- [ ] Social entrepreneurship
- [ ] Social media
- [ ] Supervisor
- [ ] Technology provider
- [ ] Trading platform
- [ ] Other
- [x] Not applicable

## Important notice on the publication of responses

*Contributions received are intended for publication on the Commission's website. Do you agree to your contribution being published?

(see specific privacy statement)

- (•) Yes, I agree to my response being published under the name I indicate (*name of your organisation /company/public authority or your name if your reply as an individual*)
- ( ) No, I do not want my response to be published

# 2. Your opinion

## 1. Fostering access to financial services for consumers and businesses

FinTech can be an important driver to expand access to financial services for consumers, investors and companies, bringing greater choice and more user-friendly services, often at lower prices. Current limitations in traditional financial service markets (e.g. opacity, lack of use of big data, insufficient competition), such as financial advice, consumer credit or insurance, may foreclose access to some categories of individuals and firms. New financial technologies can thus help individuals as well as small and medium-sized enterprises (SMEs), including start-up and scale-up companies, to access alternative funding sources for supporting their cash flow and risk capital needs.

At the same time, potential redundancy of specific back-office functions or even of entire market players due to automation via FinTech solutions might have adverse implications in terms of employment in the financial industry, even though new jobs would also be created as part of the FinTech solutions. The latter, however, might require a different skill mix.

Question 1.1: What type of FinTech applications do you use, how often and why? In which area of financial services would you like to see more FinTech solutions and why?

Member firms use FinTech applications and/or technologies for a variety of purposes. This includes, amongst others:

General products / services:
• End-to-end digital banking – The ability to open an account and complete the majority of transactions on a mobile phone.
• Investment advice and self-directed investing – Online vehicles for both individual retirement and non-retirement accounts, providing easy-to-use (and inexpensive) automated advice, as well as enabling our customers to buy and sell stocks and bonds, etc. (again inexpensively).
• Electronic trading and other online services (e.g., cash management) in our Corporate & Investment Bank and Asset & Wealth Management businesses – Offering our clients a more robust digital platform.

Cloud Technology:
• Internal/Private Cloud: the internal cloud provides developers with rapid agility, allowing for more time on developing as opposed to provisioning infrastructure and application services.
• Public cloud: Public cloud reduces peak infrastructure requirements by providing compute services during temporary fluctuations in demand. Furthermore, it also helps reduce long-term storage costs and accelerates developer access to cloud services.

Application Programing Interfaces (APIs): we estimate that by end-2017 our applications will generate 100 million internal and external API calls each day.
• Internal API stores can provide access to marketplace of secure application services to internal developers. The ‘Old world’ of developing and writing unique code is being replaced by reusable component pieces (“micro services”) that can communicate seamlessly. This reduces integration development time

and improves developer efficiency.
• External API: Expanded APIs offered externally to enable direct client integration and secure solutions by third-party developers.

Data analytics / Big Data: New technologies allow us to access and analyse data in ways that we could not have done before. For example, providing a more holistic view of a firms risk exposure.
Robotics:
• Robotic automation software automates routine, repetitive activity that would otherwise be performed manually. Actual bots available 24/7 to efficiently execute simple processes without the risk of human error - e.g. automating systems access administration.
• Such benefits will allow us to position workforce around higher-value tasks and functions.
Machine Learning: Machine learning technology provides insights about data without needing to pre-program algorithms, and actively learns from data with the goal of predicting outcomes.
• E.g. Contract intelligence platforms that uses unsupervised machine learning to analyse legal documents and to extract important data points and clauses.
• E.g. using machine learning to drive predictive recommendations for Investment Banking.
Cognitive automation: Cognitive automation, which combines both robotics and machine learning technologies to mimic human judgment. Cognitive automation has the potential to automate more complex, human-like processes, such as perceiving, hypothesizing and reasoning.
• E.g. Virtual assistant technology to respond to employee technology service desk requests through a natural language interface.

## Artificial intelligence and big data analytics for automated financial advice and execution

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 1.2: Is there evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services (investment services, insurance, etc.)?

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

If there is evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services, at what pace does this happen? And are these services better adapted to user needs? Please explain.

• Yes, financial advice is now available to a subset of people who had previously been excluded from investment offerings. Some of those clients may be lower down the wealth continuum where investment advice has historically been too expensive for banks and other financial institutions to provide, others may have excluded themselves from the investment process due to a lack of knowledge or felt intimidated by their perceived lack of knowledge. Better online education and transparency through automated advice will increase accessibility.
• The use of AI can allow firms to offer investment advice at lower costs and fees than traditional advisory programs, and in some cases require lower account minimums than traditional investment advisers.
• This can potentially allow firms to increase financial inclusion by making investment advisory services more affordable and accessible to consumers that may not previously have made use of these services.
• Automated financial advice can offer consumers more choice in how they manage their investments and receive advice by offering a wider range of products and services.
• Consumers can access services more easily through online and digital channels, and while important in its own right, investors can choose not to interact with human advisors if they prefer not to
• However, it may not be the most suitable solution for all consumers or investors, based on individual situations and the complexity of their needs. There are a number of hybrid models that can bridge the gap and allow the solution to better adapt to the needs of a wide range of users.

Question 1.3: Is enhanced oversight of the use of artificial intelligence (and its underpinning algorithmic infrastructure) required? For instance, should a system of initial and ongoing review of the technological architecture, including transparency and reliability of the algorithms, be put in place?

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

Please elaborate on your answer to whether enhanced oversight of the use of artificial intelligence is required, and explain what could more effective alternatives to such a system be.

• Focus should be on what AI is used for, not on the use of AI itself. This is in line with the EC's principles of technology neutrality and also recognises that AI has many applications beyond automated advice and financial services.
• As with all models and algorithms, it is necessary to implement a robust framework for documentation, development, testing, and maintenance of systems to ensure transparency and unintended consequences.
• Oversight is required from both a technology infrastructure and legal, risk and controls perspective.  Failing to provide suitable oversight will ultimately lead to negative experiences for clients across the wealth continuum, particularly in a bear market where limitations of models are more likely to be exposed.
• Incumbent banks will have controls and oversight processes and procedures in place (albeit they may need refining to deal with AI models). Furthermore, financial institutions are required to make available plain language description of algorithm assumptions to investors under the GDPR and MiFID II.
• Given the risks associated with handling and holding client assets, similar requirements should be imposed on actors providing such services, regardless of the type of company. The right balance must be found between ensuring suitable oversight, controls and regulation while not stifling innovation.
• The reliability of algorithms could be further ensured by supervisors through the use of simulations to monitor the AI system and control of methods and information used in the training of the machine.

Question 1.4: What minimum characteristics and amount of information about the service user and the product portfolio (if any) should be included in algorithms used by the service providers (e.g. as regards risk profile)?

Digital advisors should aggregate only data that is necessary to deliver their services, while ensuring compliance with existing regulations such as the General Data Protection Regulation or financial markets regulation including MiFID II suitability assessment rules and Know Your Customer requirements.

Question 1.5: What consumer protection challenges/risks have you identified with regard to artificial intelligence and big data analytics (e.g. robo-advice)? What measures, do you think, should be taken to address these risks/challenges?

Transparency into underlying investments is critical. Controls must be in place to ensure the quality of information that is delivered to clients is both accurate and timely. The use of push notifications to inform of short term changes vs long term investment objectives is one way to ensure transparency. As robos go through inevitable consolidation in the market, treatment of clients may also become a theme that needs to be addressed.

With regards to the use of big data generally, it is important to note that several existing EU legislations and/or other regulatory requirements such as the Payment Services Directive 2, the General Data Protection Regulation (GDPR), the Markets in Financial Instruments Directive (MIFID 2), etc. are expected to mitigate potential risks which could be linked to the lack of transparency, misuse of data, recognising that the difference between the use of data and big data is principally about scale. Having said this, possible risks and mitigants are as follows:

• Customer trust is vital to banks' business, requiring high levels of security and reliability. New uses of data are evaluated from the perspective of no harm to the customer and firm reputational risk review.

• It is difficult to anticipate the extent to which more risk-based credit scoring might limit credit to those who cannot afford it – this depends on the risk appetite of various financial institutions. Any decision not to extend credit would be taken in the context of sound risk management (involving human decisioning) and safety and stability.

• There is a potential for differential treatment of consumers, but this can be mitigated with proper controls, including proper de-identification and aggregation of data, and appropriate human interpretation of findings and how to apply the findings to banking practices. The human interpretation should adopt the "no customer harm" review lens and should keep in mind the Unfair Commercial Practices and Unfair Contract Terms regulations.

• Cyber risk – Any new channels for sourcing data could potentially increase cyber risks by effectively broadening the network. However, banks have demonstrated a robust and sustained commitment to ensuring the protection of customer information and integrity of financial systems and networks. Greater concern is around any requirements to allow open access to data or data sharing with third parties that may not have equivalent protections or are not subject to the same strict requirements around data security.

## Social media and automated matching platforms: funding from the crowd

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 1.6: Are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding?

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

Please elaborate on your reply to whether there are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding. Explain in what way, and what are the critical components of those regimes.

Question 1.7: How can the Commission support further development of FinTech solutions in the field of non-bank financing, i.e. peer-to-peer/marketplace lending, crowdfunding, invoice and supply chain finance?

Question 1.8: What minimum level of transparency should be imposed on fund-raisers and platforms? Are self-regulatory initiatives (as promoted by some industry associations and individual platforms) sufficient?

## Sensor data analytics and its impact on the insurance sector

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 1.9: Can you give examples of how sensor data analytics and other technologies are changing the provision of insurance and other financial services? What are the challenges to the widespread use of new technologies in insurance services?

Question 1.10: Are there already examples of price discrimination of users through the use of big data?

- [x] Yes
- [ ] No
- [ ] Don’t know / no opinion / not relevant

Please provide examples of what are the criteria used to discriminate on price (e.g. sensor analytics, requests for information, etc.)?

In general, firms already tier or differentiate between clients based on information available. For example: (i) trading clients might be tiered A / B / C based on their relationship and business size, with each of these tiers receiving different pricing as well as a different level of service; or (ii) in the insurance industry where rates are set based on a number of factors such as gender and wealth bracket, amongst others. All of this requires data, and the use of big data analytics means that it is occurring at a larger scale. The possible risks of big data, and means by which those risks might be mitigated, have been addressed elsewhere in our response, including in Q1.5.

## Other technologies that may improve access to financial services

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 1.11: Can you please provide further examples of other technological applications that improve access to existing specific financial services or offer new services and of the related challenges? Are there combinations of existing and new technologies that you consider particularly innovative?

• In general, technology is changing the financial service landscape with more convenient, affordable products and services. We are seeing new products developed, and new mechanisms of product and service delivery, that reach vulnerable consumers at scale.
• Promising FinTech approaches are using behavioural science principles, such as reminders and commitment devices, to nudge people to make better decisions.
• Additionally, FinTech is using data to improve our understanding of consumers to design better products tailored to consumers' needs, such as hybrid products that connect savings and spending, or products that help consumers to address mismatches between consumption and income patterns.
• FinTech has also enabled products that include customized and action-oriented information, in contrast to generic financial information campaigns that often do not lead to behaviour changes.
• Technology alone will not address financial insecurity. To ensure the adoption and usage of FinTech products requires delivery through trusted intermediaries, such as non-profit and community partners, which allows for human interaction.

## 2. Bringing down operational costs and increasing efficiency for the industry

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

FinTech has the potential of bringing benefits, including cost reductions and faster provision of financial services, e.g., where it supports the streamlining of business processes. Nonetheless, FinTech applied to operations of financial service providers raises a number of operational challenges, such as cyber security and ability to overcome fragmentation of standards and processes across the industry. Moreover, potential redundancy of specific front, middle and back-office functions or even of entire market players due to automation via FinTech solutions might have adverse implications in terms of employment in the financial industry, even though new jobs would also be created as part of the FinTech solutions. The latter, however, might require a different skill mix, calling for flanking policy measures to cushion their impact, in particular by investing in technology skills and exact science education (e.g. mathematics).

Question 2.1: What are the most promising use cases of FinTech to reduce costs and improve processes at your company? Does this involve collaboration with other market players?

Some of the most promising use cases of Fintech, that are being developed in partnership with other market players, to reduce costs and improve processes are:
• Cloud computing technology – allows cost reduction, flexibility and scalability to respond faster to customer requests through a better use of IT resources,
• Robotic automation software – automates routine, repetitive activity that would otherwise be performed manually and 24/7 execution of simple processes without the risk of human error
• Machine learning technology – provides insights about data without needing to pre-program algorithms, and actively learns from data with the goal of predicting outcomes.
• Cognitive automation – combines both robotics and machine learning technologies to mimic human judgment. Cognitive automation has the potential to automate more complex, human-like processes, such as perceiving, hypothesizing and reasoning. E.g. Virtual assistant technology to respond to employee technology service desk requests through a natural language interface.
• Distributed Ledger Technology (DLT) – has the potential to reshape financial services infrastructure, DLT may facilitate transfers of assets between parties without depending on a trusted intermediary to provide centralization of data or workflows.

Question 2.2: What measures (if any) should be taken at EU level to facilitate the development and implementation of the most promising use cases? How can the EU play its role in developing the infrastructure underpinning FinTech innovation for the public good in Europe, be it through cloud computing infrastructure, distributed ledger technology, social media, mobile or security technology?

• A one-size-fits-all regulatory approach is not conducive to technology innovation. Any new regulatory framework should be flexible, graduated and principle-based. Oversight should be tight to scale and the risks presented.
• The European Commission and Member States have a role to play in promoting interoperability as a public policy goal, helping to map new priorities and fostering companies’ technology contributions to standardisation. The market-led approach has achieved enormous success and this models needs to be preserved, including in the global context.
• A careful assessment is, however, needed in order to avoid conflicting standardisation on big data, cloud and cyber security.

Question 2.3: What kind of impact on employment do you expect as a result of implementing FinTech solutions? What skills are required to accompany such change?

• The net impact of new technologies in general has been positive, but we should acknowledge that technology does cause some job loss, dislocation and disruption in specific areas. Retraining is the best way to help those disrupted by advancements in technology.
• Automation of repetitive activity, which would otherwise be performed manually, may allow for the workforce to be positioned around higher-value tasks and functions.
• This requires re-skilling of existing employees, in particular with respect to digital skills. We also expect that employees with specific competences on ICT, science, technology, engineering and mathematics will be required.

## RegTech: bringing down compliance costs

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 2.4: What are the most promising use cases of technologies for compliance purposes (RegTech)? What are the challenges and what (if any) are the measures that could be taken at EU level to facilitate their development and implementation?

RegTech has the potential to transform the way financial institutions manage the regulatory environment, allowing them to be more efficient and dynamic in their response to new requirements and expectations.

We believe that the most promising use cases of technologies for compliance purposes are:
• Identifications of clients and legal persons (including ultimate beneficial owners) for the purpose of Know-Your-Customer (KYC) requirements
• Real-time transaction reporting to regulators including for anti-money laundering/ counter-terrorism financing purposes
• Fraud prevention
• Automation of compliance reporting

There is scope to speed up innovation in RegTech in financial services through the adoption of regulatory sandbox-like partnerships, allowing regulators to closely monitor a RegTech firm’s operations in a limited-scale, safe harbor, regulatory environment. Such structures should be encouraged at EU level through the exchange of good practices.

## Recording, storing and securing data: is cloud computing a cost effective and secure solution?

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 2.5.1: What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services?

• Financial institutions' use of public cloud solutions remains restricted due to inconsistencies and ambiguities in supervisory expectations relating to cloud outsourcing and requirements of using systems, controls, processes and procedures designed for traditional outsourcing arrangements.
• For example, it would be helpful to clarify criteria against which the materiality of a specific public cloud technology or service can be considered to help determine when outsourcing rules will apply.
• Compliance with GDPR rules on cross-border –and data flows to subcontracted third parties (including cloud service providers and their vendors) is also a significant barrier for banks entering wholesale into the cloud.
• Requirements for the mandatory localization of financial and fiscal information within the territory of individual Member States are restricting financial services firms' ability to contract cloud computing services.
• Another key factor slowing down cloud adoption in the banking industry is the lack of an internationally harmonized regulatory framework, which creates inefficiencies, particularly for banks operating with a global presence and with global consumers. The EC should work with international bodies towards a global convergence.
• Considering all of the above, we welcome the EBA's recently published guidance consultation on outsourcing to the cloud service providers.

Question 2.5.2: Does this warrant measures at EU level?

- [x] Yes
- [ ] No
- [ ] Don't know / no opinion / not relevant

Please elaborate on your reply to whether the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services warrant measures at EU level.

• Clarification of regulatory guidance aimed at the financial industry sector would help banks quantify their risks and build viable cloud strategies.
• To this end, we welcome  the European Banking Authority's consultation on proposed guidelines regarding for the use of cloud computing services, as it seeks to clarify supervisory expectations within the EU. Furthermore, we would also welcome the development of general contract term models for specific types of cloud initiatives. This could make early approval feasible, taking into account cloud service providers' certifications and the findings of assessments or audits performed by the supervisors.
• We would also welcome the lifting of any data localisation obligations as part of the 'free flow of data initiative' to facilitate centralised cloud data infrastructure strategies, and therefore believe it can also help to clarify that the right to access and audit cloud data is more important than data location.

Question 2.6.1: Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with?

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

Please elaborate on your reply to whether commercially available cloud solutions do meet the minimum requirements that financial service providers need to comply with.

• Significant cloud service providers engaged with financial firms need to be able to demonstrate their own, and their supply-chain, equivalent of appropriate financial services policies, standards, control objectives and controls prior to contracts being approved.
• However, this can be very challenging and specific risk acceptances may also be required, especially in ensuring compliance with all global regulations for the financial services firm.
• Regulators are increasingly seeking that, in absence of direct control of regulated financial services, contractual languages should reflect these requirements.
• This is not always possible or understood by the cloud service provider whose commodity based approach is not suited to bespoke and differing requests from different jurisdictions, A more centralized set of requirements as per 2.5. would aid all parties.

Question 2.6.2: Should commercially available cloud solutions include any specific contractual obligations to this end?

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

Please elaborate on your reply to whether commercially available cloud solutions should include any specific contractual obligations to this end.

• Besides the cloud service provider’s operative responsibility around service provisioning, banks as data controllers are liable for the data stored and processed. As such, cloud consumers need assurance that all contract terms are fulfilled.
• However, some CSPs are not always able to comply with specific contract terms, such as the right to audit. Pre-approved contract templates for specific use cases would be useful to facilitate compliance with a commonly understood set of minimum requirements to operate in Europe.

## Disintermediating financial services: is Distributed Ledger Technology (DLT) the way forward?

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 2.7: Which DLT applications are likely to offer practical and readily applicable opportunities to enhance access to finance for enterprises, notably SMEs?

We believe that DLT disruption of existing business models could result in enhancing access to finance for enterprises, including:
• Supply chain finance - Invoice financing could grow exponentially once the invoices are identified/ marked over DLT (when coupled with counterparty identity and credit risk attached to the invoice), and would also be trading in a secondary market.
• Trade finance - DLT can ensure that all parties can see and transfer shipping and trade documentation through a secure decentralized network, eliminating many of the current inefficiencies in international trade. Therefore, DLT could speed up trade transactions, reduce costs for companies around the world and reduce the risk of documentary fraud.

Question 2.8: What are the main challenges for the implementation of DLT solutions (e.g. technological challenges, data standardisation and interoperability of DLT systems)?

• DLT is a nascent technology. To date, proof of concepts of DLT solutions are relatively small in scale and often isolated. The main challenge is identifying compelling business cases around specific DLT applications, and at the same time having a critical mass of network participants.
• Secondly interoperability with existing infrastructures and adoption of common standards by all relevant market players is required to make DLT applications more scalable.
• Thirdly, DLT solutions can only materialize if technological and governance challenges including with respect to data and protocol standardization, security and error recovery are addressed.
• The nature of DLT means that DLT errors will be common to all participants at the same time, as the ledger errors are synchronized to all participants. This highlights potential risks around governance of a DLT network, such as membership criteria, membership vetting, certification, consensus mechanisms, certificate authority, standards ownership, identity management and supervisory participation.

Question 2.9: What are the main regulatory or supervisory obstacles (stemming from EU regulation or national laws) to the deployment of DLT solutions (and the use of smart contracts) in the financial sector?

In general, as policymakers consider DLT within the context of the regulatory and supervisory framework the following should be taken into account:

• DLT is at an early stage of development and deployment. Therefore, it is important that any regulatory approach to DLT does not implicitly limit or constrain firms' ability to test and develop DLT solutions. Further, we support a regulatory framework that treats all current and future industry participants on an equal and fair basis, so that as DLT re-shapes the market, barriers to entry are not created that could negatively impact adoption and innovation.

• The potential uses for DLT are numerous and diverse. Any regulatory framework needs to be sufficiently cognizant of the diverse potential applications of DLT that are adaptable to operating across multiple activities and services. Consequently, the adoption of a “one size fits all” regulatory framework for DLT is unlikely to be effective.

• If a situation arises where the use of DLT poses challenges within a certain regulation, policymakers should take a pragmatic approach to such situations. The possibility of DLT not fitting within certain regulations should not be viewed negatively, given that the current regulatory framework was not developed with a technology like DLT in mind.

• Regulate the specific application, not DLT: While there may be aspects of the regulatory framework relevant to DLT as a technology platform, this is distinct from applying a regulatory framework to regulated financial activity that utilizes DLT.

Divergent regulatory approaches to DLT in different jurisdictions may hinder the adoption of DLT in an optimally beneficial way. To this extent, we would urge regulatory cooperation and international harmonisation to enable an effective and facilitative DLT framework. There is perhaps a role for CPSS-IOSCO to set overall standards, noting its work on the Principles for Financial Market Infrastructures (PFMIs).

## Outsourcing and other solutions with the potential to boost efficiency

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 2.10: Is the current regulatory and supervisory framework governing outsourcing an obstacle to taking full advantage of any such opportunities?

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

Please elaborate on your reply to whether the current regulatory and supervisory framework governing outsourcing is an obstacle to taking full advantage of any such opportunities.

```
The current regulatory and supervisory framework governing outsourcing is too prescriptive and is out of date. It appears to have been prepared on the assumption that firms would outsource activities completely, on an end-to-end basis. However, firms often use technology solutions as “building blocks” to create larger solutions. Some of the building blocks may be retained within the firm and others provided by third parties. The current regulatory and supervisory framework needs to be amended to give firms more flexibility in how they manage the risks associated with using external service providers.
```

Question 2.11: Are the existing outsourcing requirements in financial services legislation sufficient?

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

Please elaborate on your reply to whether the existing outsourcing requirements in financial services legislation are sufficient, precising who is responsible for the activity of external providers and how are they supervised. Please specify, in which areas further action is needed and what such action should be.

```
The UK FCA general outsourcing requirements provide a high barrier to entry for material outsourcings to FinTechs.  However, this is ultimately necessary to ensure customers can be confident of the banks’ ability to manage this new technology.  There could certainly be more done at an industry level to assist with common standards and processes for assessing and on-boarding FinTech companies and smaller technology providers as suppliers to large banks.
```

## Other technologies that may increase efficiency for the industry

Question 2.12: Can you provide further examples of financial innovations that have the potential to reduce operational costs for financial service providers and/or increase their efficiency and of the related challenges?

# 3. Making the single market more competitive by lowering barriers to entry

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

A key factor to achieving a thriving and globally competitive European financial sector that brings benefits to the EU economy and its society is ensuring effective competition within the EU single market. Effective competition enables new innovative firms to enter the EU market to serve the needs of customers better or do so at a cheaper price, and this in turn forces incumbents to innovate and increase efficiency themselves. Under the EU Digital Single Market strategy, the EU regulatory framework needs to be geared towards fostering technological development, in general, and supporting the roll-out of digital infrastructure across the EU, in particular. Stakeholder feedback can help the Commission achieve this goal by highlighting specific regulatory requirements or supervisory practices that hinder progress towards the smooth functioning of the Digital Single Market in financial services. Similarly, such feedback would also be important to identify potential loopholes in the regulatory framework that adversely affect the level playing field between market participants as well as the level of consumer protection.

Question 3.1: Which specific pieces of existing EU and/or Member State financial services legislation or supervisory practices (if any), and how (if at all), need to be adapted to facilitate implementation of FinTech solutions?

Question 3.2.1: What is the most efficient path for FinTech innovation and uptake in the EU?

• The EU FinTech ecosystem is strong and growing with the current level of regulatory engagement. As the FinTech ecosystem continues to evolve, regulators should monitor for emerging risks and take action when warranted, while ensuring there are no constraints on collaboration between institutions. Engagement beyond this may have unintended consequences.
• More active involvement could be beneficial for educational purposes (especially for FinTechs seeking partnerships with banks or other financial institutions), which in turn will help foster effective environment for innovation.

Question 3.2.2: Is active involvement of regulators and/or supervisors desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants?

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

### FinTech has reduced barriers to entry in financial services markets

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

### But remaining barriers need to be addressed

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 3.3: What are the existing regulatory barriers that prevent FinTech firms from scaling up and providing services across Europe? What licensing requirements, if any, are subject to divergence across Member States and what are the consequences? Please provide the details.

• Each member state has different regulatory bodies with different regulatory appetites and different laws. In general, we encourage regulatory harmonisation and passporting across Europe. In addition we encourage a global approach working with other jurisdictions outside of the EU.

Question 3.4: Should the EU introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market?

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

Question 3.5: Do you consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market?

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

If you do consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market, please explain in which areas and how should the Commission intervene.

• We support the development of an EU framework for experimentation, akin to the FCA regulatory sandbox, especially for new entrants.  We also support a global approach given the cross-border nature of experimentation.
• These are safe spaces in which both incumbents and new players can test innovative products, services or business models in real world environments with guidance from the regulator with the potential to do so without full compliance with applicable regulations. This approach enables a more forward-looking assessment by financial supervisors and could ultimately lead to new regulatory and supervisory approaches
• We believe that if structured correctly as outlined in 3.8, regulatory sandboxes have the potential to facilitate robust dialogue between banks, non-banks FinTechs and regulators on deploying innovative services and technologies. It is important that authorities do not stifle innovation of established financial institutions, and therefore should allow their voluntary participation in regulatory sandboxes.
• We believe that the development of an EU framework for regulatory sandboxes will help avoid fragmentation of the market and could facilitate intra-EU cross-border expansion of successful FinTech projects.

Question 3.6: Are there issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market?

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

Please elaborate on your reply to whether there are issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market, and explain to what extent regulations on data localisation or restrictions on data movement constitute an obstacle to cross-border financial transactions.

• Various financial services cross-national borders e.g. payments and other services provided to multinational businesses.
• Localisation mandates and preferences take many forms, including regulations, certification/accreditation, administrative requirements, procurement policies, and regulatory guidance, many of which are sector-based. They also include, for example, laws based on national security requirements (e.g., for classified data), company record laws, and archival requirements (requiring storage of records in a specific institution inside a country).
• The impact of data localisation is significant: data localisation complicates cross-border business strategies, bans and restricts market access, limits choice of service provider, can limit access to data, limits access to new technologies e.g. cloud, increases costs, adds red tape, adds legal uncertainty, creates misconceptions that localisation provides for better security, and introduces the possibility of bias into models as large groups of observations may not be included as input data.
• Restrictions on the flow of data within Europe (and around the world) affect the digital single market. While data localisation measures may be justified in limited circumstances (e.g. confidential government data), their impact on the growth of the European data economy is generally negative: they fragment the single market and raise costs for the deployment of cross-border data economy services. Such measures have a particular impact on the infrastructure underlying the data economy - such as cloud services - because these services require major investments which cannot feasibly be made on a country-by-country basis.

Question 3.7: Are the three principles of technological neutrality, proportionality and integrity appropriate to guide the regulatory approach to the FinTech activities?

- [x] Yes
- [ ] No
- [ ] Don’t know / no opinion / not relevant

Please elaborate on your reply to whether the three principles of technological neutrality, proportionality and integrity are or not appropriate to guide the regulatory approach to the FinTech activities.

Yes, the three principles are broadly appropriate.

As noted in cover letter, As the EC considers its policy approach to FinTech, it should keep in mind the following:
• A one-size-fits-all regulatory approach is not conducive to technology innovation - any new regulatory framework should be flexible, graduated and principles-based, and oversight should be tied to scale and the risks presented;
• Any new rules or guidance should take into account banks' existing authorities to develop, test and launch innovative products and services. It's also important that regulators do not implicitly limit the ability to experiment - new initiatives will not always work and that is OK;
• Regulators / supervisors should develop expertise, engage both banks and nonbank innovators, and focus frameworks on functions, not specific technologies or companies; and
• FinTechs have the ability to operate across jurisdictions. New regulatory and supervisory frameworks to address FinTech innovation should aim to be harmonious with existing innovation frameworks in order to mitigate against regulatory arbitrage and conflicting rule sets that stymie the development of innovative products and services.
• We support consistent, activities-based standards for FinTechs and emerging business models. Regardless of the type or scale of company, certain activities - i.e. payments, lending, data storage, wholesale infrastructure development - warrant the same regulatory requirements because of the significance of the associated risks (e.g. AML/ KYC, terrorist financing, fair lending, privacy, unauthorized data use, cyber security) posed to consumers and the broader financial system.
• Cyber security is a good example of this principle. A failure by any single market participant hurts the reputation and damages trust in the industry as a whole.

## Role of supervisors: enabling innovation

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 3.8.1: How can the Commission or the European Supervisory Authorities best coordinate, complement or combine the various practices and initiatives taken by national authorities in support of FinTech (e.g. innovation hubs, accelerators or sandboxes) and make the EU as a whole a hub for FinTech innovation?

• We support the regulatory sandbox concept, especially for new entrants, and believe that if structured correctly, it has the potential to facilitate dialogue between banks, nonbank FinTechs, and regulators on the barriers to partnerships or marketing of innovative services/technologies.
• We believe participation should be voluntary for established financial institutions, as there are already robust controls and risk management processes in place.
• We welcome a Europe-wide approach to sandboxes- e.g. harmonised criteria for entry, simple and transparent authorisation process - to avoid un-level playing field and to facilitate successful innovations are implemented across Europe with the minimum delay.
• Having said this, we recommend that that the European Commission consults on the design and structure of an EU-level regulatory sandbox before introducing any such initiative.

Question 3.8.2: Would there be merits in pooling expertise in the ESAs?

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

Please elaborate on your reply to whether there would be merits in pooling expertise in the European Supervisory Authorities.

Question 3.9: Should the Commission set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns?

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

If you think the Commission should set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns, please specify how these programs should be organised.

• In general, we are supportive of collaboration between industry and policymakers in particular with respect to cyber security.
• Cybersecurity collaboration is essential. The financial services sector is not an "island unto itself"—there are critical dependencies on entities that provide energy, water, telecommunications, computing, etc.
• Key cybersecurity collaboration opportunities include expanding the quality and scope of information sharing, working with suppliers to improve third party oversight, and strengthening the resiliency of systemic utilities and exchanges.

Question 3.10.1: Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS?

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

Please elaborate on your reply to whether guidelines or regulation are needed at the European level to harmonise regulatory sandbox approaches in the MS?

We welcome a Europe-wide approach to sandboxes- e.g. harmonised criteria for entry, simple and transparent authorisation process – to avoid un-level playing field and to facilitate successful innovations are implemented across Europe with the minimum delay. Having said this, we recommend that that the European Commission consults on the design and structure of an EU-level regulatory sandbox before introducing any such initiative.

We believe common principles should be considered for:
• Clear and simple conditions for experimentations;
• Security, consumer protection and competition rules safeguards;
• Access for all suppliers both regulated businesses and non-regulated businesses;
• Education with guidance on the interpretation of the legislation in relation to the testing activities
• No enforcement action/infringement procedures during the testing phase
• Exit and transition strategy should be clearly defined in the event that the new solution has to be discontinued, or can proceed to be deployed on a broader scale
• Participation should be voluntary for established financial institutions, as we already have robust controls and risk management processes in place
• Ex-post assessment

Question 3.10.2: Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border?

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

If you would see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border, who should run the sandbox and what should be its main objective?

We welcome a Europe-wide approach to sandboxes- e.g. harmonised criteria for entry, simple and transparent authorisation process - to avoid un-level playing field and to facilitate successful innovations are implemented across Europe with the minimum delay. Having said this, we recommend that that the European Commission consults on the design and structure of an EU-level regulatory sandbox before introducing any such initiative.

We believe common principles should be considered for:
• Clear and simple conditions for experimentations;
• Security, consumer protection and competition rules safeguards;
• Access for all suppliers both regulated businesses and non-regulated businesses;
• Education with guidance on the interpretation of the legislation in relation to the testing activities
• No enforcement action/infringement procedures during the testing phase
• Exit and transition strategy should be clearly defined in the event that the new solution has to be discontinued, or can proceed to be deployed on a broader scale
• Participation should be voluntary for established financial institutions, as we already have robust controls and risk management processes in place
• Ex-post assessment

Question 3.11: What other measures could the Commission consider to support innovative firms or their supervisors that are not mentioned above?

## Role of industry: standards and interoperability

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 3.12.1: Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision?

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

Please elaborate on your reply to whether the development of technical standards and interoperability for FinTech in the EU is sufficiently addressed as part of the European System of Financial Supervision.

• We do not believe that the European System of Financial Supervision (ESFS) needs to play a more proactive role in the development of standards. There are however opportunities to promote global standards in a way to support competition, risk management and interoperability.
• By its very nature, FinTech often includes products and services that are not jurisdiction-specific – such as data processing, cross-border payments, settlement reconciliation. It would therefore almost always be counterproductive to seek to move towards anything other than global standards.

Question 3.12.2: Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities?

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

Please elaborate on your reply to whether the current level of data standardisation and interoperability is an obstacle to taking full advantage of outsourcing opportunities.

Question 3.13: In which areas could EU or global level standards facilitate the efficiency and interoperability of FinTech solutions? What would be the most effective and competition-friendly approach to develop these standards?

• FinTechs have the ability to operate across jurisdictions. New regulatory and supervisory frameworks to address FinTech innovation should aim to be harmonious with existing innovation frameworks in order to mitigate against regulatory arbitrage and conflicting rule sets that stymie the development of innovative products and services.
• As global regulatory bodies (FSB/IOSCO/Basel) continue to monitor this space, they should help coordinate FinTech-focused policies from member jurisdictions such as the EU.

Question 3.14: Should the EU institutions promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses?

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

Please elaborate on your reply to whether the EU institutions should promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses, and explain what other specific measures should be taken at EU level.

• This does not appear to be an appropriate role for EU Institutions. Technology service providers and other owners of intellectual property can choose whether to make their solutions available on an open source basis.

## Challenges

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 3.15: How big is the impact of FinTech on the safety and soundness of incumbent firms? What are the efficiencies that FinTech solutions could bring to incumbents? Please explain.

• FinTech, considered generally, can improve safety and soundness by reducing errors and making the firm more efficient. Big data analytics, for example, can allow firms to re-engineer their Market Risk platform delivering a more granular and holistic view of the firms risk exposure.
• Collaborating with FinTech companies can also bring efficiencies and improved services/products, by connecting external ideas with incumbent knowledge, data, space and other resources to co-create solutions.

## 4. Balancing greater data sharing and transparency with data security and protection needs

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 4.1: How important is the free flow of data for the development of a Digital Single Market in financial services? Should service users (i.e. consumers and businesses generating the data) be entitled to fair compensation when their data is processed by service providers for commercial purposes that go beyond their direct relationship?

• In general, current and forthcoming data protection legislation provides consumers with adequate protections and greater transparency into how their data is used and ability to consent and opt-out, and also ensures that service providers do not process data for purposes that go beyond the purposes for which the data were collected. This provides appropriate protection, limiting the need for a system of compensation in return for data use.
• It may be important to articulate benefits of analytics to clients /customers. Such benefits include offering of new, more personalized, and/or less expensive products – e.g. robo-advisory products, offering personalized investment advice, for consumers in wealth brackets for which the offering was previously not available (either as a product or due to the high cost).

### Storing and sharing financial information through a reliable tool

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 4.2: To what extent could DLT solutions provide a reliable tool for financial information storing and sharing? Are there alternative technological solutions?

• The financial services industry already has a range of tried and tested solutions for storing and sharing financial information. New technology and process are constantly reviewed to assess whether they can provide efficiencies or improve services.
• DLT is no exception and the financial industry has been investigating the potential merits of this technology for several years. It is not a panacea, but there are some specific use cases where DLT might offer reliable solutions. So far many of the most useful solutions have appeared in the post-trade environment, however, over time we expect to see other solutions making use of DLT technology.
• For example, there are many financial processes and services that could benefit from the immutable nature of DLT storage. Customer data, contract information, property rights, and in general "digital fingerprints" of any kind of agreement (even when signed off the ledger) are some of the types of information that could be stored in a DL.
• We see DLT as complementary to APIs. DLT is generally better for pushing or broadcasting data, APIs are good for pulling data. DLT by itself is not really suited to be an information store, but is good for data synchronisation between multiple organisations.

Question 4.3: Are digital identity frameworks sufficiently developed to be used with DLT or other technological solutions in financial services?

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

Please elaborate on your reply to whether digital identity frameworks are sufficiently developed to be used with DLT or other technological solutions in financial services.

• Digital identity may be difficult for certain use cases. However, it is important to note that there will be a number of use cases for which it is not an issue e.g. institutional use cases, of which digital identify frameworks at the individual/end investor level are currently not a significant obstacle for the development of DLT applications. For retail use cases and eventual interoperability or merging between institutional & retail DLT platforms, current digital identity frameworks may require further development.
• Member States have should fully embrace the regulatory opportunity created by the eIDAS Regulation. On the one hand the notification, mutual recognition and cross-border interoperability of the various member states' public eID schemes is taking time to achieve. On the other, the conditions for the commercial usability of the various national eID frameworks remain diverse and fragmented. The Commission, ENISA and the European Standardisation Organisations should pursue their already significant efforts further to encourage member states to make their national schemes interoperable and to open them up to wider and easier commercial use.

Question 4.4: What are the challenges for using DLT with regard to personal data protection and how could they be overcome?

• Data held within DLT is very likely to be encrypted.  However, with continuous increases in computing power and technology advances, we assume that any encryption applied today will be compromised in the future, maybe in 3 years, maybe 20 years.
• Therefore, we would treat DLT the same as any other technology in regard to personal data protection.  Personal data should only be shared with parties that have explicit permission to see the data, regardless of encryption
• For DLT this leads to two scenarios that can be applied to data sharing: (1) The DLT does not hold personal data, but may hold pointers to where the data is held. (2) The DLT supports scenarios where the data elements are only shared with a specified subset of network participants, not all participants.
• There are various forms of DLT solutions, including solutions where the data is accessible only to users who have been given appropriate access. The existing legal and regulatory framework provides sufficient protection. To introduce regulatory requirements specifically for DTL solutions would be contrary to the Commission's stated objective of being technology neutral.
• Restrictions on transfer of data across national borders potentially creates a challenge for use of DLT solutions. However, the same applies to other technology solutions, e.g. cloud computing solutions.

## The power of big data to lower information barriers for SMEs and other users

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 4.5: How can information systems and technology-based solutions improve the risk profiling of SMEs (including start-up and scale-up companies) and other users?

• Start-up and scale-up companies are very difficult to risk profile. Each is unique and requires extensive work to understand the business, hence it is also very difficult to make comparisons.
• However, big data technologies may allow more information to be acquired from SMEs, reducing the credit risk and financial risk. The Internet of Things could also support acquisition of data on the assets of SMEs and improve risk profiling.
• On achieving more risk-based credit scoring, we agree that while it could improve credit conditions for some users, in some cases it could involve denying credit to those that cannot afford it. If data is unreliable then results might not be accurate and customer detriment could result. Overall, any innovative use of customer data for lending purposes should be consistent with responsible lending principles

Question 4.6: How can counterparties that hold credit and financial data on SMEs and other users be incentivised to share information with alternative funding providers ? What kind of policy action could enable this interaction? What are the risks, if any, for SMEs?

## Security

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 4.7: What additional (minimum) cybersecurity requirements for financial service providers and market infrastructures should be included as a complement to the existing requirements (if any)? What kind of proportionality should apply to this regime?

• Financial institutions are heavily investing in their IT systems including cyber-security measures. Cyber-security is particularly relevant when FinTechs collaborate with financial institutions, as end-to-end security across the whole financial services chain must be ensured.
• Technology innovations – including Internet of Things, artificial intelligence and cloud – open the door for increasingly complex cyber threats. Therefore, any solution offered by FinTechs based in new technologies should be built with privacy and security considerations by design.
• Effective cyber defence requires a global perspective. These efforts require collaboration and partnerships to counter innovative threat actors and evolving risks. As such, financial firms must collaborate with government, other financial industry partners, as well as vendors and clients around the world to effectively address cyber threats.
• We support regulatory harmonization by global supervisors around risk-based approaches to cybersecurity risk management. We support adopting the G7 "Fundamental Elements of Cybersecurity for the Financial Sector" as a starting point for all cybersecurity regulation; we consider the NIST framework to be an example of an instantiation of the principles defined in the G7 "Elements".

Instead of legislation, promoting, encouraging and harnessing business innovation through new tools such as cyber-insurance and self-certification regimes, would be a constructive way to improve the adoption of cybersecurity best practices by stakeholders of all sizes and of all cyber maturity levels. Approaching cybersecurity in a risk-based manner is key to ensure effective resilience throughout the supply chain.

Question 4.8: What regulatory barriers or other possible hurdles of different nature impede or prevent cyber threat information sharing among financial services providers and with public authorities? How can they be addressed?

• All players, including FinTechs, should be able to share on a cross-border level cyber threat intelligence and cyber incident information through reliable and safe tools and mechanisms in order to increase cyber resilience. Firms often collaborate with other members of the financial industry beyond interaction with governments and regulators. The belief that cybersecurity is not a competitive issue has allowed the industry to work together to improve the cyber defences of the sector as a whole. Information sharing and coordinated analytic work have been the hallmarks of sector collaboration. We support the rules as drafted in the EU Network and Information Security Directive and calls on national governments to ensure consistent implementation of the Directive.

• Having said this, the two main obstacles to meaningful cyber threat information sharing remain the lack of robust liability safeguards for the information that is disclosed, and the lack of reliable control mechanisms for information originators post disclosure. Taking these two issues in turns: (1) Very often, to be relevant, timely and actionable, cyber threat intelligence will need to include information the disclosure of which may be restricted under applicable regulatory provisions (e.g. privacy rules applicable to personal data such as network identifiers of compromised computing resources). Unless these regulatory restrictions are explicitly waived, or unless the disclosing party is explicitly cleared from liability for disclosing such information to the extent and in the circle strictly necessary for the purpose of improving collective cybersecurity, effective cyber threat information sharing will be deterred. These obstacles are for the legislator to address in the relevant regulatory instruments. (2) Once cyber threat information has been volunteered, precisely because its relevant, timely and actionable nature make it highly sensitive, it is still important to ensure that the originating party remains in control of how the information is subsequently accessed, used and further disseminated, and that the originating party does not end up being held liable for any mismanagement or undue processing or disclosure of the information by others.

• For these reasons, in AmChamEU members’ experience, a key differentiator between successful threat information sharing mechanisms and unsuccessful ones is the existence and effective use of a robust information classification and access control mechanism (such as the Traffic Light Protocol – TLP) to manage information shared by participants. This is a matter of adopting and implementing best practices by the participants of the various relevant information sharing schemes. ENISA has developed ample guidance and reference materials on these matters.

• A legal construct akin to the Joint Money Laundering Intelligence Taskforce (JMLIT) would also provide full legal cover to allow for greater cyber security information sharing at national and EU level.

• The creation of a unique point for cyber incident reporting and subsequent harmonisation of differing reporting formats and procedures under the GDPR, NIS Directive and PSD2 will also streamline the sharing of information among market players and authorities.

• Finally the focus should not only exclusively be on improving cyber defence (predict, prevent and protect) but also on making it risky to be a cyber-criminal (prosecute).

Question 4.9: What cybersecurity penetration and resilience testing in financial services should be implemented? What is the case for coordination at EU level? What specific elements should be addressed (e.g. common minimum requirements, tests, testing scenarios, mutual recognition among regulators across jurisdictions of resilience testing)?

• Penetration tests by third parties introduce operational and data risks. We support firms conducting their own penetration tests in partnership with the regulators, based on the framework GFMA has developed.
• We are supportive of EU level penetration testing if done correctly, i.e. along GFMA guidelines, to the extent that it would further regional coordination. We are also supportive of a safe and scalable approach to regulatory penetration testing and red teaming across the entire EU wherein single test results satisfy multiple supervisors' requirements (limiting the operationally risky execution of penetration tests or red team assessments).

## Other potential applications of FinTech going forward

Please refer to the corresponding section of the consultation document to read some contextual information before answering the questions.

Question 4.10.1: What other applications of new technologies to financial services, beyond those above mentioned, can improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing?

Question 4.10.2: Are there any regulatory requirements impeding other applications of new technologies to financial services to improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing?

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

Please elaborate on your reply to whether there are any regulatory requirements impeding other applications of new technologies to financial services to improve access to finance, mitigate information barriers and/or improve quality of information channels and sharing?

## 3. Additional information

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

**71ba92ce-3483-4fe0-94e5-ab131a3b96eb/Statement.pdf**

### Useful links

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

Consultation details (http://ec.europa.eu/info/finance-consultations-2017-fintech_en)

Specific privacy statement (https://ec.europa.eu/info/sites/info/files/2017-fintech-specific-privacy-statement_en.pd

### Contact

fisma-fintech@ec.europa.eu