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:

Barclays

Contact email address:

The information you provide here is for administrative purposes only and will not be published

roeland.vanderstappen@barclays.com

*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:

72390466359-39

*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?

United Kingdom

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

at least 1 choice(s)

- [ ] Accounting
- [ ] Asset management
- [ ] Auditing
- [x] 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
- [ ] 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?

Barclays' Accelerator programme allows us to enter into a process of reasonable length to understand Fintech start-ups proposition and work with them to develop their company and product so that we might be able to integrate their services.

Financial Technological innovations are more and more developed by banks with open processes that include customers, suppliers, outsourcers and start-ups.

It is worth pointing out that banks do a lot of fintech themselves, in the meaning of developing innovative, technology based financial solutions and services.

We see concrete benefits to enhance specific key business areas, products and/or services by leveraging:

- solutions focused on cost reduction via improvement to processes or replacement of platforms/ IT solutions with either new business models or technologies; ;
- solutions enabling banks to attract and on-board new customers, to improve customers' relationship or to increase the offer of new and innovative products/services
- risk management;
- cybercecurity (e.g. fraud detection and data protection);
- regulatory (regtech).
- current processing solutions in the payments or securities space. Allowing the testing of new technologies such as Distributed ledgers is of paramount importance.

Banks also have a lot to offer to Fintech startups, in particular, specific financial expertise (risk assessment, evaluation and management), scalability owing to their large customer base, as well as many years of experience in providing clients with regulatory-driven high levels of operational security. All of this is in addition to the substantial financing solutions offered by banks. The complementary strengths and weaknesses of both banks and Fintech startups mean that both will often do better by cooperating rather than by competing.

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.)?

- (●) 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.

> Innovation in artificial intelligence and big data analytics is driving the development of sophisticated forms of automated financial advice, including robo-advisors.
>
> Robo-advice has already had a significant impact on the wealth management industry. It allows to significantly lower the price of financial advice, while offering consumers a wide range of choice in terms of services and customization capabilities. Therefore, robo-advice allows to reach the mass-affluent market that has traditionally been underserved.
>
> More broadly digital tools, when combined with human advisors, can provide new and scalable means to bridge the increasing advice gap.
>
> Controls are important to ensure quality of advice. The provenance of the advice should always be clear (and if the respondent is human or machine or both).

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.

We do not believe that enhanced oversight of artificial intelligence is needed at this stage, and would consider that regulating outcomes as the best approach in this area and in line with the principle of technology neutrality.

Financial institutions and other providers of automated financial advice tools already put in place a number of measures to ensure that the use of artificial intelligence and its underlying algorithm deliver financial advice that is well calibrated and tested before it is used in the market.

This includes the close involvement of human advisors in the design and oversight of automated advice tools, to ensure that the algorithm delivers the expected outcome.

Under the General Data Protection Regulation, financial institutions are required to satisfy accountability and transparency requirements and therefore the use of artificial intelligence will be subject to privacy impact assessment and oversight.

The reliability of algorithms could be further ensured by supervisors through the use of simulations to monitor the artificial intelligence system and control of methods and information used in the training of the machine.

This would also require a greater consideration of digital skills in the selection of staff among regulators and supervisory authorities to review financial institutions' technological architecture.

We would welcome a standard definition of quality of outcome measurement as well as process controls that ensure human SME-knowledge has control on the outcome.

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)?

We do not believe that enhanced oversight of artificial intelligence is needed at this stage, and would consider that regulating outcomes as the best approach in this area and in line with the principle of technology neutrality.

Financial institutions and other providers of automated financial advice tools already put in place a number of measures to ensure that the use of artificial intelligence and its underlying algorithm deliver financial advice that is well calibrated and tested before it is used in the market.

This includes the close involvement of human advisors in the design and oversight of automated advice tools, to ensure that the algorithm delivers the expected outcome.

Under the General Data Protection Regulation, financial institutions are required to satisfy accountability and transparency requirements and therefore the use of artificial intelligence will be subject to privacy impact assessment and oversight.

The reliability of algorithms could be further ensured by supervisors through the use of simulations to monitor the artificial intelligence system and control of methods and information used in the training of the machine.

This would also require a greater consideration of digital skills in the selection of staff among regulators and supervisory authorities to review financial institutions' technological architecture.

We would welcome a standard definition of quality of outcome measurement as well as process controls that ensure human SME-knowledge has control on the outcome.

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.

We expect constant development in this space for the foreseeable future as technology moves from initial development to maturity. Therefore, we believe it is more appropriate for regulators to focus on outcomes, rather than algorithms, in order to ensure customers are protected and treated fairly.

We believe it is too early to consider new regulatory measures as several existing EU legislations, including the General Data Protection Regulation (when it becomes enforceable in May 2018) and MiFID II, are already expected to mitigate potential consumer protection risks that could be linked to the lack of transparency, misuse of data, suitability assessments and consumers being 'locked-in'.

We would support a certification of cognitive engines, the monitoring of training activities and the monitoring use of applications to ensure liability of each actor involved in the given service (e.g. cognitive engine provider, system integrator that trained the machine, company offering the service, user himself).

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.

Recital 47 of GDPR has specific provisions in relation to profiling for prevention of fraud and tax evasion, but explicitly expanding this to include cybersecurity and defence of financial services and payment systems would improve the ability of the implementation of AI solutions in the Security arena.

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?

- 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.)?

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?

> The use and application of Distributed Ledger Technology and 'smart contracts' can potentially enhance specific business areas within banks as well as the IT core banking system.
>
> For example, Barclays processed the world's first live trade finance transaction via blockchain in September 2016. The transaction facilitated the export of goods using distributed ledger technology developed by our partner Wave, a graduate of the Barclays Accelerator programme. The platform uses distributed ledger technology to ensure that all parties can see, transfer title and transmit shipping documents and other original trade documentation through a secure, decentralised network, eliminating many of the current inefficiencies in international trade and reducing the time taken for transactions to complete from 10+ days to just over four hours.
>
> ISDA's new initiative on the standardisation of data and processes for derivatives smart contracts, as announced at ISDA's 2017 AGM. Note that Barclays publicly demonstrated a proof-of-concept in April 2016 comprising the negotiation of ISDA smart legal agreements on Barclays' prototype user interface and the execution of the corresponding smart contract code on R3's prototype Corda distributed ledger platform.

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:

- Digitalisation of processes that facilitate the interaction with customers
- Cloud computing, the aim of which is cost reduction, flexibility and scalability to respond faster to customer requests through a better use of IT resources
- AI/Big data use can tailor financial products and services to meet consumers' needs as well as facilitate better risk management and regulatory compliance.
- Financial services robotics process automation can help reduce costs and increase quality through scalable solutions
- Distributed Ledger Technology (DLT) has the potential to reshape financial services infrastructure. DLT may facilitate transfer of assets between parties without depending on a trusted intermediary to provide centralization of data or workflows.
- Standardisation of business logic
- Utility settlement token to support instantaneous settlement of trades
- Cryptography to establish secure communication for financial services

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 and varying interpretations on for instance big data, cloud and cyber security and ensure that standardisation does not introduce systemic weakness into an environment or market.

Development of regulator accepted industry standards for cloud computing which align to other areas of regulation (such as GDPR, PSD, NIS) would provide a strong joined-up narrative. It's sub optimal to leave individual Fintech/FIs/NBFIs to interpret the high-level guidance which currently exists at the national level.

It would be useful if the EU took a leadership role in developing standards and security requirements, and in defining the rules for items like segregation of access, network security, data protection, incident response, portability across providers, etc..

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?

Whilst the digitization and automation in the banking industry will reduce costs it will not necessarily lead to an overall reduction in employment. FinTech and bank collaboration and the implementation of FinTech solutions can create new market opportunities and subsequently create new jobs.

However, financial firms face the challenge to re-skill existing employees, in particular with respect to digital skills. We also expect that employees with specific competences on ICT, data science, technology, engineering, cybersecurity 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
- Matching relevant regulation to internal policy and/or standard to furthermore understand the control impact on the organisation
- Horizon scanning opportunities to help understand if something is likely to become regulation before it actually does

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.

Ultimately it would be good if there was standardization around regulation e.g. unique blockchain DNA identifier which we could trace all the way through the regulatory lifecycle (from regulator through to effective control

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 because of challenges of understanding how to meet legal and regulatory requirements using systems, controls, processes and procedures designed for traditional outsourcing arrangements.

These include lack of 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 data protection laws on cross-border transfers-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.

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.

In the short term, CSPs should seek to specifically address the guidance prescribed by the PRA/FCA. Longer term, there is a need to join up industry standards like the CSA (Cloud Security Alliance) with regulators to develop finance industry approved standards that CSPs can attest to. Building a strong relationship between regulators and the CSP's is likely to significantly aid adoption.

Question 2.5.2: Does this warrant measures at EU level?

- (●) 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.

Therefore, we welcome the European Banking Authority's consultation on proposed guidelines for the use of cloud computing services, as it seeks to clarify supervisory expectations within the EU.

Furthermore, we would 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?

- ○ 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.

Uncertainties pertaining to compliance with certain regulatory requirements, such as outsourcing requirements regarding effective supervision and oversight of cloud service providers and their supply chains, challenge a proportionate risk-based approach to due diligence.

The auditing of outsourced services to the cloud is particularly complex. Banks are required to cooperate with regulators and generally secure (on-site) access rights to records, premises and personnel. In addition, for cloud providers to operate at the scale they do, requires automation, conformity and homogeneity of approach across their client base. Thus if a cloud provider was to allow each financial services company the right to audit, it would create a significant burden on the cloud provider. Moreover, it is often a point of tension in negotiations with cloud service providers, who are reluctant to allow customers into their data centres for legitimate security and confidentiality reasons.

Furthermore, in a globalized and distributed cloud model, access to the physical locations delivers a negligible outcome. This challenge is further driven by an ambiguity how far auditing rights should be exercised throughout the supply chain.

It would be useful if attestations and detailed reviews could be performed at an industry level in harmony with regulators, ensuring CSPs are meeting the necessary controls and removing the need for each organisation to re-audit the same standard components.

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

- (●) 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.
>
> Further considerations include regulating CSPs to established security standards where they provide services for material outsourcing of financial institutions and establishing liability for security breaches which are the fault of the CSP.
>
> Cloud services pose a number of challenges in relation to their relative maturity in terms of flexibility in providing greater control to financial services organizations than most of their users. This is especially true with respect to cryptography and level of control and security demands expected of financial institutions.

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.

Finally, clarification the regulatory framework with respect to DLT solutions is needed. The ambiguity of regulation results in the industry being concerned about retrospective fines.

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?

It is important that any regulatory approach to DLT does not implicitly limit or constrain firms' ability to test and develop DLT solutions.

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.

We do believe that the further development of DLT solutions requires clarification of the legal framework with respect to:

o Legal validity of documents stored in the DLT as proof of possession or existence

o Legal validity of financial instruments issued on the DLT

o Enforceability and liability of smart contracts & legal certainty of settlement finality securities traded on the DLT

o Treatment of shared information in DLT from a data protection perspective, in particular with respect to interpretation of 'right to erasure' in a tamper-proof blockchain environment.

o Regulatory reporting information standards on the DLT

Divergent regulatory approaches to DLT in different jurisdictions may hinder the adoption of DLT in an optimal way. To this extent, we would urge regulatory cooperation and international harmonisation to enable an effective and facilitative DLT framework.

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?

- (●) 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?

```
Regulatory handbooks, particularly on outsourcing rules, should be amended
to give regulated firms more flexibility in how they manage the risks
associated with the use of FinTech solutions.
```

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

We support the regulatory sandbox concept, especially for new entrants, and believe that, if structured correctly, it has the potential to facilitate robust dialogue between banks, non-bank FinTechs and regulators on policy barriers to partnerships or deploying innovative services and technologies.

For example, regulators should get involved in the testing of multi-bank DLT projects where the regulator could observe its “regulator node” - that could provide useful learnings for the regulators.

A level playing field is needed to ensure fair competition between financial institutions and FinTech players. Therefore, 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 (AML/KYC, terrorist financing, fair lending, privacy, unauthorized data use, operational continuity) posed to consumers and the broader financial system.

In an increasingly open banking environment, as a result of PSD2, it is key that all parties are certified as secure and regularly audited and supervised. Security should not be underestimated as open banking may potentially open up to bigger security breaches than experienced so far, increasing risks. Therefore, it is key to establish EU-wide robust standards, controls and monitoring to prevent higher risks for customers.

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

If active involvement of regulators and/or supervisors is desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants, please explain at what level?

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. We encourage regulatory harmonisation, standardization, passporting and lower barriers to entry across Europe, implemented through a framework, rather than regulation. 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

If the EU should 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, please specify in which specific areas you think this should happen and what role the ESAs should play in this. For instance, should the ESAs play a role in pan-EU registration and supervision of FinTech firms?

We support the use of licensing and passporting to facilitate FinTech businesses to operate across borders, while ensuring a balanced framework and security in areas that are unregulated (e.g. digital assets, crowdfunding).

At the same time, these licenses should be specific for the activity that the FinTech companies want to perform, to ensure effective supervision of their risks. A closer supervision by the authorities is required to ensure that the services provided by those companies remain under the provisions of that they have been licensed for. Further the type of service providers in transactions should be classified.

Financial institutions should also be provided a fast-track framework that allow them to develop digital solutions at the same pace as new entrants. In both cases, all participants should contribute to financial stability, consumer protection and cybersecurity measures. Proportionality should be applied in a way that ensures the application of these principles, based on the risks and activities, rather than on the size or nature of the service provider.

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, 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.

Data localization requirements create serious challenges from an information sharing perspective also in the context of Financial crime activities (including money laundering, fraud, sanctions screening, KYC, terrorist financing, PEPs); compliance with Financial Services Regulatory obligations (e.g. MiFID, MAR, 4AMLD etc); disclosure of information to local and foreign law enforcement.

The GDPR introduces more stringent requirements for businesses in many areas but at the same time it continues to provide for a high level of freedom in moving personal data between organisations. To ensure that a free flow of data is pursued, there is a need for a greater certainty and harmonization. For example, in the context of US-EU data transfers, many US firms opted for not relying on the Privacy Shield due to uncertainty as to its future, continuing to rely instead on model clauses. If these clauses are also challenged, in the way that Safe Harbor was, this would present a fundamental barrier to the financial services industry, which by its nature involves regular and significant cross-border flows of data.

Data localization requirements are also at odds with trends in technology. The latter, unlimited by geographic boundaries, can manage storage and access to data, globally. However, certain Member States have introduced, at national level, additional limitations and barriers which prevent data circulation and intra-group synergies at EU and international level. While, Member States' interests in law enforcement and national security are fully legitimate, there is no valid justification for data localization. Local law banking secrecy and client confidentiality should be looked at separately from the provision of security to those solutions.

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

- (●) 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.

> 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 idea of implementing a "regulatory sandbox" within the EU to encourage firms to test innovative products, services and business models without immediately being subject to the usual regulatory requirements. That being said, we also understand that an EU-level regulatory sandbox as such would be challenging because the supervision generally remains at national level.
>
> However, we welcome global 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 and other jurisdictions with the minimum delay.
>
> A Fintech incubator, coordinated by the European Supervisory Authorities and promoted by the European Commission, could be an excellent opportunity to collect new ideas, identify new innovative services, monitoring trends and addressing the innovation especially in the perspective of potential regulatory adjustments and integrations. In addition we would support a global response co-ordination body.

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

- ○ Yes
- ○ No
- ◉ 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?

- (•) 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.

The European Commission could draw on best practices from Member States including the BoE Fintech Accelerator or FCA FinTech bridges.

We would welcome an “Innovation Academy” set up by the European Commission in association with other regulators/policymakers from non EU jurisdictions, coordinated by the ESAs and supported by financial (and non-financial) associations (both in the EU and non EU jurisdictions), could help to train subject matter experts with common background, able to spread the Fintech’s culture of innovation and to promote the development of innovative solutions.

We also welcome improved dialogue on FinTech discussions within existing fora such as the European Data Protection Board (EDPB), ENISA as well as the European Supervisory Authorities.

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

- (•) 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 believe national approaches are not helpful in a multinational and global financial industry. The main risk of a national approach might be to create a fragmentation with different approaches among the EU Member States, with the final result that neither financial institutions nor consumers can benefit from these initiatives.

We welcome a global 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 and non EU jurisdictions with the minimum delay.

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
- 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?

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

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

Sandboxes should not only consider the mechanism for ensuring the technologies can prevent harm to the market, but may also wish to consider both how the solution can be protected and the relative merits of the security of the product being tested in the sandbox.

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.

The current level of data standardisation and interoperability is an obstacle to taking full advantage of outsourcing opportunities. Trade Associations are one possible route for helping to formulate solutions.

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?

> In the context of FinTechs, the objectives of efficiency and interoperability can only be enabled by standards if they are developed at a global level, are outcomes based, technology agnostic, transparent, and inclusive. We believe that existing mechanisms (e.g. the ISO governance and procedures for developing and maintaining new and existing standards) or work within international fora (e.g. IOSCO, FSB) and European and international trade associations can provide for this.

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.
>
> We would however advocate the use of a community that can develop open source solutions. In particular, we note that there is no consolidated 'rule book' in Europe. It would be helpful to promote adherence to standards, rules and obligations in a more open approach to highlight the obligations on developers, particularly when using standards.

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.

```
        Where incumbents are able to on-board technology solutions (whether
through M&A or commercial relationships) which allow them to remedy issues
created by complex legacy systems and manual processes, this is likely to be
a big driver of efficiency.  However, as per above, the process is not always
easy for regulatory compliance reasons.
        At the same time, FinTech solutions can potentially build legacy
systems on top of legacy systems.  It is important to note that new
technology is not always the answer.
```

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?

```
        Unjustified national data localisation requirements should be
addressed under the ‘free flow of data initiative’ to facilitate centralised
(cloud) data infrastructure strategies. The EU-US Privacy Shield as well as
EU model contractual clauses are needed to provide legal certainty for
transatlantic data flows.
        Current and forthcoming data protection legislation appropriately
restricts service providers from processing data of service users for
purposes that go beyond the purposes for which the data were collected
(purpose limitation). This is an adequate protection for service users.
        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.

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 is arguably one of the most important aspects to successful DLT adoption. In a distributed network environment Digital Identity is of paramount importance to ensure trust. Without trust, DLT implementations will fail.

Digital identity frameworks today are evolving, but not yet fully ready to meet the demands of many potential DLT use cases. We think that lack of adequate Identity Frameworks is a key blocker to successful DLT adoption. The same is true for wider API adoption. The UK financial services industry is currently working on this to meet the challenges of Open APIs operating in an environment where consumers are protected against rogue and fraudulent actors.

In addition there is a need to clarify the regulatory framework with respect to the liability of data sharing.

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:

- The DLT does not hold personal data, but may hold pointers to where the data is held.
- 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.

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. In this context, the implementation of GDPRand PSD2 should offer a significant opportunity to design APIs that are built applying the highest standards of privacy by design and security.

It is equally important that third party vendors and third parties accessing bank infrastructure in an open banking/ PSD2 context are certified as secure and regularly audited and supervised.

Together with the new requirements in the NIS Directive, and the developments in cyber laws in the US and elsewhere, further cyber legislation is not necessarily required. A focus on ensuring consistency between, and compliance with, existing requirements is likely to be more beneficial.

We support regulatory harmonization by global supervisors around risk-based approaches to cybersecurity risk management.

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.

Barclays already participates in a number of differing bodies where cyber threat intelligence is shared, such as FSIISC, FIISAC and other industry bodies, including ones where closer information-sharing occurs such as the Cyber Defence Alliance.

There are challenges in certain jurisdictions in relation to data privacy in respect to what is personally identifiable information (e.g. IP address) which not only makes information-sharing difficult but also makes monitoring to prevent activity problematic. The recently introduced exclusion for prevention of fraud within GDPR should be extended to cybersecurity prevention and monitoring.

New requirements on GDPR inhibit or provide obstacle to appropriate monitoring of insider threat and collaboration with law enforcement, government agencies and wider industry.

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

The focus should not 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)?

Barclays operates a robust, intelligence-led and threat-centric penetration testing program, as well as operates a series of desktop and technical tests designed to assess the resilience of our key systems globally. We also have a robust Global Supplier Assurance team who carry out broader assessment of the risks of our suppliers.

Coordination at an EU level would help to determine the level of testing required to satisfy regulatory expectations across multiple jurisdictions, which could then be used as a minimum bar for developing our test program.

There may be an opportunity for harmonisation of the testing of financial institutions and FinTech aligned to the frameworks that existence in the UK such as CBEST. Sector specific cyber wargaming such as “Waking Shark” may enable improved understanding for regulators of the capabilities of market participants and also sector level improvements.

We are lacking necessary controls on large established software companies introducing vulnerabilities globally.

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:

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