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:

German Banking Industry Committee

Contact email address:

The information you provide here is for administrative purposes only and will not be published

f.zuther@bvr.de

*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:

52646912360-95

*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?

Germany

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

at least 1 choice(s)

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

*Please specify your activity field(s) or sector(s):

```
Our members are active in every imaginable field of finance - including
fintec startups
```

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?

Banks provide payment, banking/financial management tools (Webservices Apps APIs) for their customers. The average customer uses an ATM once a month (almost 100% of customers), the webservice twice a week (80% of users) and the banking app almost daily (20% of customers).
Banks use technology-enabled innovation along almost the entire process chain. Examples for applications are:

- Video-chat based customer identification
- Personal financial planning (PFM) / multi-bank aggregation
- Semi-automated account switching tools
- Information capturing and structuring for transaction orders
- Robo advice
- Digital Asset Management
- deposit aggregation
- mobile payments
- …

Giving a comprehensive overview about existing financial technology solutions used by the banking industry is not possible, primarily due to the lack of a common definition: that is to say, the difficulty in drawing a clear line between what is considered financial technology and what is not.
We would like to see more financial technology in the area of administrative services around money management, such as APIs for tax or other e-government purposes that accept the banks' identification of customers, to provide better overall services.
In addition, the area of Entrepreneurial- and SME Finance Management has potential which has yet to be fully exploited. For example (robo-) accounting, cashflow predictions or even e-government solutions, can spur entrepreneurial spirit and increase firm foundations.
Furthermore, potential for financial technologies in the area of foreign trade financing should be spurred. This may reduce the administrational boundaries in import- and export finance as well as for customs duties.

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.

Not actual evidence, but a lot of potential in the field.

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.

The use of big data and artificial intelligence is at a very early adoption stage by financial service providers. Therefore, regulation should not be put in place before it becomes obvious that conceivable risks are likely to materialise. Existing rules and regulations should be applied to the new technological options; adjustments should be made wherever an examination indicates an actual need to do so.
The oversight has to ensure that artificial intelligence is not the only way for decisions to be made, but there is a right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
Regulation should be on an equal footing for any intelligence, whether it is artificial or human. It must also be ensured that the same regulatory framework for (product) recommendations is met – by banks as well as by third parties. As the PSD2 requires banks to grant registered Third Party Service Providers (especially account information services) access to a customer’s bank account data, new market participants have a data basis at their disposal which is comparable to the basis that account-keeping banks have today. It is to be expected that Third Party Service Providers will also use this data for individual customer recommendations.

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)?

Depending on the specific service, human advisors are already obliged to ask clients for specific information, and to take that into account when giving advice. The same should apply for automated advice.

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?

A more algorithm-based analysis of consumer data has the clear potential to improve consumer and investor protection and promote financial stability. A broader base of data will enable a customer's personal situation, such as his /her risk appetite or temporary financial difficulties, as well as his capacity in terms of understanding the products and the risks involved, to be better and more promptly identified. The customer can then be contacted and an appropriate course of action can be recommended. This could enable consumer and investor protection to be designed more effectively than current instruments allow. Better knowledge of customers also has positive effects on a bank's risk management, and thus on financial stability in general.
While appreciating the benefits of big data in risk assessments, it should be considered that predictions from big data are probably the best alternative, but they do not claim to be perfect and cannot be made the only basis for decisions.
We can in particular envisage two situations where Big Data prognosis reaches its limits:
a. Due to "black swan" (events so rare that we do not have valuable statistical material [yet]) and/or
b. Faults or biases in algorithms that cannot be detected within the regular (test-)data, or due to the learning aspect within the algorithms
The judgement on human behaviour should be based on human understanding, human reasoning and causality, not only on correlation. Human reasoning should always be more valued than machine reasoning, and an appropriate rate of exceptions to machine reasoning needs to be implemented within the guidance rules of all companies. This is especially true in advice, since all machine reasoning assumes the future to be like the past - if a human makes use of his free will to change more drastically, machine advice may not be suitable for that situation.

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.

Apparently, the German Kleinanlegerschutzgesetz has shown some impact since it entered into force in 2015: There has been a consolidation of the crowdfunding sector; no further remarkable growth, and no striking negative examples either. A recent study commissioned by the German government came to the conclusion that one third of the crowdfunding volume has been used for property financing. As a broad variety of financial solutions already exisit in this financing segment, it is not necessary to have less strict financial regulation in comparison to property financing by banks.
Important components of a regulatory regime are: eligible assets, thresholds for volumes, transparency requirements.

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?

The commission can install a bureau for legal clearance for all innovative firms, or ideas to clarify the regulatory needs for innovative ideas. That way the commission will be aware of new ideas and their regulatory problems, while innovators will benefit from accountable information.

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?

This depends on the service/business model. Transparency to protect the customer is regulated in the financial sector quite profoundly - the risk needs to be understood by the investor, and also needs to be comparable to other options.

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.)?

Risk-based pricing of loans has longstanding history in the financial sector, and is even prudentially promoted. It is an example of price discrimination based on the criteria of default risk. To our knowledge, the use of big data - in the sense of unstructured data stemming from social media platforms or other external sources - is still very limited today.

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?

```
By using mobile devices, customers receive improved overview and control of
their finances (e.g. access to their account or to payment details at any
time, real-time collection of the transaction history in the case of mobile
payments).
Instant credit application via smartphone allows for ad-hoc financing when
required (e.g. impulse purchases/bargains) and thus more flexibility for the
customer whilst simultaneously assessing his/her creditworthiness.
Bitcoin wallets make anonymous payments possible - online as well as on site.
Cash withdrawals at retail points of sale facilitate the access to cash, thus
reducing infrastructure costs for banks and retailers alike.
```

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?

```
Fully automated self service 24/7 is already is a big cost saver. Cash
withdrawals at retail points of sale may make matters easier for market
entrants, as they will avoid the trouble of having to establish their own
dedicated infrastructure. Blockchain and or crowdfunding may be used in
disintermediating the market of money supply and demand, or the market of
asset transfer and storage, especially worldwide (as ripple does with swift).
```

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?

The first key for such a market evolution would be non-discriminatory access to technical or infrastructural components of the digital age, because financial services are becoming increasingly dependent on these technical aspects:

- messaging services need to be designed to be usable in such cases:
  - pseudonymous address book matching
  - sufficient encryption to protect privacy of financial facts
  - non-discriminatory access for enterprise use
- mobile infrastructures such as NFC antenna or fingerprint scanner, system integrity, advanced (passive) authentication processes need to be accessible

The second key for such a market evolution would be in customer protection. Markets need to evolve in such a way that the trust of customers is always justified. A level playing field needs to be implemented, taking into account risk adjustments and full risk transparency for the customer.

To meet the demands of banks and customers in a digital age, a full digitisation and simplification of onboarding procedures at EU level should be facilitated. Due to KYC/AML requirements, financial service offerings require a prior identification of the customer which is costly and time-consuming, since digital solutions are not available in practice. In this regard, we support the aim of the European Commission to facilitate the cross-border use of electronic identification and know-your-customer portability. We are however skeptical that the eIDAS framework is able to provide an appropriate solution for the private sector, at least in the mid-term. Instead we advocate a more open and market-driven regime with regard to the underlying technology. A conceivable approach could be – for instance – a regime whereby banks could rely on past identifications provided by other banks. With such an approach, customers would only go through an identification procedure once at their bank (“as trusted party”); other banks or third party service providers then should be allowed to identify their customers by using the trusted party’s data. A legal basis would have to be provided for this process; liability issues regarding a proliferation of errors are especially crucial.

Many specialised fintech enterprises develop products, and operate according to business models which are subject to statutory permissions – in Germany in accordance with the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz – ZAG) or the German Banking Act (Kreditwesengesetz – KWG). Since the application for such a license generally involves significant organisational efforts and financial expenditure, the application for an own license following the commencement of operations is – in most cases – not worth considering for specialised fintechs. Instead, many such companies depend on cooperations with established banks, in order to ensure compliance with the regulatory framework and all obligations of their business models. It should thus be as simple as possible for banks to enter such cooperations by promoting the latter, in order to strengthen the innovatory power of the financial sector as a whole.

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 demand for customer service, as well as back-office workers, will
decrease. However, the need for personnel with higher education and skills in
data mining (e.g. software engineers, data scientists etc.) will increase. On
the business/product side, employment has to change to a mix of experts and
specialists who are aware of creative and technological developments with a
focus on consumers.
```

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?

```
The methods of automated testing, availability analysis etc. could be used by
the regulator to secure availability and trust in public services without
interference of banks' daily routines.
Blockchain could be another valuable technology. In our opinion, the DLT can
be used for regulatory reporting purposes, assuming that regulators have
installed (and will maintain) a node for them within the DL. In this case for
instance, all settlement-related information would be available to
regulators, and there would be no need for dedicated feeds with associated
reconciliation problems. Regulators would have access to the golden record in
real time. Previously implemented regulations highlighted data quality issues
faced by the industry due to different interpretations. In relation to trade
reporting obligations, it should be noted that our response focuses on
settlement-sided aspects only - we cannot comment from a trade repository
perspective. We can, however, imagine that the DLT could cover or be used for
various (including trade-related)  types of reporting. Depending on the
design and configuration of the DLT and on the information included,
reporting in general will be facilitated by the use of the DLT. Reporting
obligations can be disposed of as far as the information needed is contained
in the DL. The challenges associated with reporting via a DLT include issues
concerning data protection, cyber security (as the regulator holds the access
to all data on the DL, it might itself become a target for cybercrime
attacks). Therefore, the set-up may have to be view-only, which can be
addressed in a permissioned set-up (only).
```

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?

Key challenges for banks present themselves in the response to the question as to what risks arise from cloud computing services. Communications, as well as the storage and 'indestructibility' of data, need to be safeguarded using technical means – with regulatory requirements to be adhered to in addition. At present, considerable uncertainty reigns amongst banks. No-one knows how supervisory authorities will assess the cloud computing process from a supervisory point of view. In addition, no uniform supervisory regulations regarding cloud computing exist within the EU. Supervisory practice shows that supervisory authorities closely scrutinise computing issues, taking related risks and the banks' risk management into account. In the event of sub-outsourcing (establishing so-called 'outsourcing chains'), banks must ensure extensive operational transparency. In the end, external procurement of cloud services could become more difficult – and expensive – for banks. Just recently, the EBA launched a Consultation on recommendations on outsourcing to cloud service providers (EBA-CP-2017-06), the results of which are intended to clarify the related problems.

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.

The Commission should await the consultation results (EBA-CP-2017-06, Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No. 1093/2010), before taking any further steps.

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.

(Unfortunately,) not only rules and regulations are essential, the supervisory practice established at the banks also plays an important role. In some cases, this practice may be significantly stricter than for other 'ordinary' market participants.

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.

-

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?

The examples given in box 1 of the questionnaire require no further additions.

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)?

In essence, the main challenges can be sorted into four areas:
- Technological issues (e.g. scalability, interoperability, central bank money, recourse mechanism, position netting)
- Governance and privacy issues
- Regulatory and legal issues
- Reach/acceptance (no specific DLT problem, but invoked by the complete new approach).

Specific questions include the following:
- Which civil law and supervisory adjustments are necessary?
- Does the procedure have to be backed by government institutions?
- Can the required amount of transactions be settled?
- Will decentralised blockchain technology be run in parallel (and be operational) to the current central register management simultaneously, or will we see a fixed changeover date? Would the systems be interoperable?
- How can cybersecurity be assured? Is it sufficient if manipulations are deemed unlikely, but not impossible? How will cryptographic advancement be achieved (crypto migration)?
- Does the identity of the participants have to be known, and can transactions be allocated to participants?
- Will business models have to be revised or realigned (e.g. services in connection with the issue, trading and settlement of securities)?

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?

We feel that regulators / supervisors should be involved at a very early stage. This will eliminate / reduce the risk of regulatory impediments to globally evolving innovation. The analysis of concrete regulatory provisions will depend on the actual envisaged application of the DLT. One general problem is at the interface of the DLT to the "real" world: Identification of the customer (certificates / digital signage)
We see specific potential regulatory impediments to the deployment of the DLT; for instance, in securities markets.
As a general rule, we would like to point to different national legal concepts of securities and safekeeping/custody of securities. Different civil laws or legal concepts should not lead to a preference for certain markets or jurisdictions because the regulatory view or interpretation of the law is more open and innovation-friendly. International harmonisation of regulation applied to securities markets could be of help.
Regulatory rules which do not necessarily focus on the way securities markets work could also pose obstacles - such as, for instance, rules on data privacy and data retention. If an obligation to delete certain (digital) data after a certain period of time were to be applied despite the data being technically needed, this could pose an impediment to ledgers under the DLT, as the DLT is based upon blocks of transactions stored in a chain and is therefore fully dependent on the complete set of all transaction data in the ledger. An obligation to delete certain data would destroy the concept of the DL. A similar challenge exists regarding the different timeframes of retention rules throughout different jurisdictions. Furthermore, the situation of nodes in the DLT in multiple legal jurisdictions will raise conflict-of-law issues. Even with one contractual law, these may prove hard to manage, particularly when referencing to the SFD.
It should, moreover, be assessed whether CSDs will still be the central position in the new DLT system. In this context and as a more concrete example, Article 3 of the CSDR could be seen as a regulatory impediment to securities traded on a trading venue, as it requires such securities to be recorded in book-entry form in a CSD. Article 18 of the CSDR could also be a potential impediment if a DL is considered to be a designated securities settlement system (SSS).

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.

Supervisory practice presents an obstacle, at least in Germany: German supervisors have general reservations regarding outsourcing activities. Even though the MaRisk only slightly restricts outsourcing activities, thus making cloud computing per se possible, the supervisory practice thwarts this - in parts, on a massive scale. Regarding cloud computing, initial experience is available as to how supervisory authorities manage it in practice. A valid assessment however is not possible, as only a small number of cases exist and it is a somewhat 'young' discipline. Considering the experience gained in the past, it is highly probable that initial efficiency gains realised via cloud computing could be lost (or even be more than offset) in the applied assessment practice at a later time - due to a re-tightened (national) regulatory framework. (Key word: retained organisation) Outsourcing requirements must be adopted in such a way that operational implementation issues are clarified directly between the regulator and the provider. Otherwise, this specialist knowledge would have to remain within the bank, making collaborative outsourcing unfeasible.
General speaking, taxes represent a significant hurdle to outsourcing (esp: Umsatzsteuer in Verbünden).

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.

Existing outsourcing requirements in the euro area are (so far) unsatisfactory, as they are scattered and thus offer too much scope of interpretation in the assessment practice. This affects the scope and flexibility within the application of existing regulations. In this context, German regulations may be seen as very extensive. In some cases, the flexibility of application is very limited or does not exist at all.
Regulations which must be observed (directly or indirectly) include: the German Banking Act (KWG), the German Securities Trading Act (WpHG), the German Capital Investment Act (KAGB), the German Insurance Supervision Act (VAG), the Minimum Requirements for Risk Management (MaRisk), the Minimum Requirements for Compliance (MaComp), the Minimum Requirements for Risk Management in Investment Companies (InvMaRisk), the German Ordinance on Audit Reports (PrüfBV), BAIT, the SREP Guideline (including the BCBS Guideline), the German Civil Code (BGB), the German Data Protection Act (BDSG), the German VAT Act (UStG), the German Private Limited Companies Act (GmbHG), the German Public Limited Companies Act (AktG), ISO, BSI, process standards (ITIL, COBIT).
Whilst cloud computing offers numerous opportunities, new, unknown and unseen risks may also occur. Thus, revising and streamlining the national and European regulations named above may be a wise decision, thus making the technological advance of cloud computing accessible for banks. This has to apply especially to small and medium-sized banks, as these are at risk of not being able to afford the implementation of cloud computing (employees, skills, costs). Outsourcing requirements must be adopted in such a way that operational implementation issues are clarified directly between the regulator and the provider. Otherwise, this specialist knowledge would have to remain within the bank, making collaborative outsourcing unfeasible.

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?

Biometrics, including “behavioural biometrics” (specific movement, typing pattern), have major potential for strong and customer-friendly authentication.
Technologies such as artificial intelligence (e.g. IBM Watson).

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?

```
1. Digital customer communications
a) Delivery assumption for electronic declarations
The submission of a declaration of intent to absent parties is subject to
section 130 of the German Civil Code (Bürgerliches Gesetzbuch, "BGB"). Unlike
with the deposit of a document in the recipient’s letter box, serious doubts
exist as to when the declarations are to be considered as received.
Declarations are often bound by expiration dates, or must be issued without
undue delay. No statutory provisions exist to date. Should the recipient
grant electronic access for declarations, as a rule it is fair to assume that
he/she will retrieve incoming messages on a daily basis. In administrative
law, however, documents are considered received after three days. Based on
this, the declaration should thus be considered received at the latest on the
third day, hereby establishing legal certainty.
b) Definition of an “adequate period of time” for the retention and storage
of information in accordance with section 126b (1) of the BGB
Many information requirements already call for text form today. In today’s
fast-growing electronic business traffic, the former model of handing over a
CD-ROM or a flash drive is outdated  Transmitting personal data to private e-
mail accounts remains a cause of concern under data protection rules.
Consumers often reject the obligation of having to print documents or
download them on their computers. Therefore, many entrepreneurs have begun to
offer electronic mailboxes on their servers. As an adequate period of time, a
```

term of four years should be provided by law (e.g. in section 126b of the BGB).
2. Digital Onboarding
At present, consumers have to individually identify and authenticate themselves whenever they establish a business relationship (registration) vis-à-vis a credit institution, financial services provider, or payment institution. In order to facilitate the onboarding process, the exchange of authentication or KYC data between obliged entities within the meaning of the German Money Laundering Act (Geldwäschegesetz – GWG) is to be made possible, meaning that the customer is not subject to renewed authentication. Therefore, the liability issues regarding the proliferation of errors have to be clarified; the regulations of section 7 of the GWG may have to be extended with specified information on the available options (such as the validity of authentication, safeguarding measures for declarations of intent on the transmission of customer data, or type and scope of the authentication data to be transmitted, etc.).
3. Digital transaction of a loan
The conclusion of consumer loan agreements still requires written form in Germany (pursuant to section 492 (1) of the BGB). The written form requirement is considered fulfilled if the application and the acceptance have been declared in writing by both parties. Signing the lender's declaration is not required if it was created using an automated system. The loan brokerage agreement entered into with a consumer is also subject to the written form requirement (section 655b (1) of the BGB).
The issue as to whether powers of attorney may be granted by way of a qualified electronic signature has not yet been fully clarified by legislators, or in legal practice. A power of attorney granted via a qualified electronic signature is not considered a letter (certificate) of attorney within the meaning of section 172 (1) of the BGB due to the lack of a physical certificate, meaning that replacement in accordance with section 126 (3) of the BGB is excluded. Alternatively, it might be argued that section 172 (1) of the BGB shall apply mutatis mutandis, meaning that the authenticity of such an electronic document is equivalent to a physical certificate.
Given the legal uncertainty, market participants have reservations regarding the acceptance of powers of attorney according to section 172 (1) of the BGB granted via qualified electronic signatures, at least in the corporate space, in order to avoid an unwanted change of communication medium. Hence, we believe it would be appropriate to require text form for granting powers of attorney according to section 172 (1) of the BGB, or to clarify in legislation that the written form requirement may be replaced by the electronic form according to section 126 (3) of the BGB.
4. Proportionality of regulatory provisions
FinTech companies often use thresholds or requirements applicable in different jurisdictions; this may lead to the application of simplified – or the waiver of – regulatory requirements. These exceptions reflect the principle of proportionality, and facilitate the market introduction of innovations. They have to apply to all market participants, in order to ensure a level playing field.
They should be maintained, and harmonised across Europe. Proportionality should not only be applied ex-post to existing business models, but should be

considered in ex-ante considerations as well.
See full answer in addendum

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

As within other fields such as telecommunications – the access to infrastructure needs to be regulated to allow new participants the entry to the market – while allowing the infrastructure providers positive business cases to further foster the needed infrastructure.
Essential infrastructures for mobile payments need to be accessible to all players in the market, and not limited to those suppliers who also provide the mobile devices. The regulator has to make sure that all payments service providers are able to access the technology components, e.g. for authentication (fingerprint scanner) or data transmission (NFC, Bluetooth Low Energy), that are required for M-Payment solutions.
In general, any form of regulation shall be neutral in terms of effects on competition, instead of being targeted at the promotion of individual business models. Monopolies and oligopolies are established in this context very easily through network effects, and need to be prevented by appropriate regulatory measures.

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.

The reasons to prevent specialised FinTech companies to provide scaling, or

offering their products throughout Europe, are in particular the lack of harmonisation of the European legislation regarding the financial sector, and the different administrative practice of supervisory authorities in the different member states (e.g. granting of licences, or establishing exceptions). These limitations also apply to established providers of financial services. This includes in particular EU Regulations where the unharmonised legal situation is created only with the transposition into national law ('gold plating' within the framework of minimum harmonisation). Room for manoeuvre granted to national governments for the implementation of EU Regulations plays another important role in this context. Differences in the legislation of member states can be observed, in particular, regarding threshold values, and simplifications or removals of certain regulatory duties – i.e. areas of law with particular relevance to specialised FinTech companies. Different legal situations in EU member states require elaborate knowledge of the respective national laws, and lead to technical and organisational product adjustments. This translates into an elevated effort in terms of time and money required for internalisation projects, representing very tough – or even unsolvable – challenges, due to personnel restrictions.
One example for inconsistent regulation is the implementation of the Anti-Money Laundering Directive (Directive (EU) 2015/847) as well as of the EU Payments Regulation (Regulation (EU) 2015/847) by the various member states:
- Acceptance of cash amounts as part of the rendering of payment services for institutions subject to the ZAG was permitted for years only as part of due diligence measures. The Third (as well as the Fourth and the Fifth) Anti-Money Laundering Directives provide for a threshold of EUR 1,000 in this context (see Article 11 (b) (ii) of Regulation (EU) 2015/849). German legislators intend to expand this excessive regulation in relation to the EU Regulation onto the German KWG, and therefore credit institutions, as part of the transposition into national law of the Fourth Anti-Money Laundering Directive. However, many other countries adopted the EUR 1,000 threshold into national law. Such an excessive regulation at a national level is in stark contradiction to the principle of equal opportunity within the EU single market, and makes internationalisation projects of FinTech companies even more difficult.
- There are also inconsistencies in the various member states regarding the threshold for due diligence requirements with respect to electronic money products, although the EU provided a threshold of EUR 250, which may even be raised to EUR 500 under certain conditions, in Article 12 of Directive (EU) 2015/847. In Germany, such exceptions are limited to due diligence measures affecting a total amount of EUR 100 or less (cf. section 25n of the KWG), while many other EU member states have adopted the threshold value of EUR 250 into national law (such as Poland and Italy).
- Even within the framework established by EU Regulations, different legal situations occur in various EU member states. For instance, the room for manoeuvre granted to national governments according to Article 2 (5) of Regulation (EU) 2015/847 is implemented differently in the EU member states. Some countries included in their respective national laws an exception for insignificant money transfers settled within one country, while other countries do not provide for such exceptions:
Österreich: Artikel 46 (3) FM-GwG and Article 8 (6) Bundesgesetzblatt Teil 1

118. Bundesgesetz
Polen: Article 9d (1) no. 1 and 2 of Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu

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.

The current regulations should be examined and revised with regard to new, digital services. In doing so, the following principles should be observed:
• The introduction of new business models should not lead to a dilution of existing consumer/investor protection rights. This enhances customer trust regarding such new business models. Hence, regulators shall provide transparent provisions for complex issues in the best interest of customers.
• A risk-adjusted level playing field must be maintained. Regulators shall provide uniform access options for different business models. Regulations should be independent from business models, i.e. new business models should be subject to requirements comparable to those applying to existing business models.

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.

Especially for cloud services banks must be able to transfer data across borders efficiently in order to respond to customers' needs. One obstacle is a lacking European or even Global regulatory framework for Cloud Computing in Financial Services. Eine Überarbeitung der hier einzuhaltenden Richtlinien aus Datenschutz etc. ist besonders für Banken sinnvoll. Different national regulation constitute a barrier to the free flow of data between different geographic locations of the physical Cloud Computing infrastructures. We also see a need to harmonize EU financial supervisors' criteria when approving cloud projects.

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 consider the three guiding principles of technological neutrality, proportionality and integrity, to be appropriate for a regulatory approach toward financial technology. With regard to proportionality, however, the principle of "same business, same risks, same rules" must not be compromised. To complement those, customer protections should be added explicitly as a fourth guiding principle.

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?

To best position the European market in digitalisation the authorities should aim at “agile regulation”. To cling to the regulatory guidelines and customer protection, risk-adjusted level playing fields need to be implemented. Therefore the regulators should seek intensive discussion and exchange – especially with innovators – and adjust regulation technology on a neutral basis to all participants in the field.
The models tested for sandboxes in Europe so far (in particular UK/FCA) still leave many questions unanswered. The following parameters shall apply to European sandboxes:
- investor protection identical to models outside of sandbox;
- risk-adjusted level playing field for providers. This requirement should be emphasised if new business models – exposed to uncertain risks – are actually launched.
- Transparency regarding the application process, and access for new, and existing, market participants.
- Processes for open discussion with all parties involved regarding the practicability, and further development, of the sandbox should be managed by regulators.
- Transparent and unambiguous framework conditions need to be established regarding an open test environment for new, or amended, financial services.
- Unambiguous transfer of business models into “normal” regulation.

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.

National regulators shall be provided with the right to implement new ways as well as own ideas within the scope of the uniform principles laid out under 3.8.1. This fosters greater dynamism, and the implementation of successful national approaches as best practice.

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.

A profound analysis needs to be carried out, the extent of which certainly goes beyond this consultation, regarding the bundling of different competences in one “Innovation Academy”.
However, we believe that positive impetus should be provided regarding the promotion of innovative digital business approaches from the institutional side. The regulatory structures currently in place focus primarily on risk avoidance aspects when dealing with financial supervisory, competition, consumer, or data-relevant issues. However, it would be desirable to implement - and integrate - the concept of economic opportunity into the regulatory structures, which would be in line with the targets defined for business and location development.

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?

The guidelines should give assurance that no problems concerning either customer protection or the risk-adjusted level playing field occur. See 3.8

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?

–

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.

–

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.

```
Required standards in the financial industry are mostly worldwide, and not
limited to EU-borders.
```

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?

```
The regulator should promote the industry standardisation processes (such as
IEEE or W3C), making sure that standards are open and can be deployed on a
non-discriminatory basis.
```

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.

```
Platforms for worldwide open source libraries already exist (github etc.). We
see no further need for promotion by the EU institutions.
However, we see a need for a platform to take insight in closed source
firmware in IoT devices such as routers, in order to approve the security or
to be able to provide patches by ourselves.
```

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.

```
Financial technology solutions providing operating efficiencies and trust can
bring significant advantages to incumbents such as banks (i.e provide trust
and execution within the settlement processbetween banks, and also with their
partners - like ripple does in worldwide exchange and settlement).
However, if infrastructure has to be opened / provided to third parties
without being able to ask for a fair compensation, this will be an
unjustified and vital loss for the incumbents. It is even more critical, if
one provider in an ecosystem has to take risks brought in by another
provider, whilst having no control of those risks. Such an environment does
not stimulate economic development, but poses incalculable risks to existing
and new business activity.
So it is a pro and con - and whilst the extent of the evolution cannot be
foreseen, it has to be managed closely.
```

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 the information age, data is the fundamental factor – in the same way that oil was in the energy age. Usage of their data should always be transparent for consumers. Natural persons should have control of their own personal data, as laid down by the framework of the GDPR. Any legitimate use of personal data by the service provider should not constitute a right for compensation.
Assessing the value of data is not a constructive approach from our view. Firstly, such an assessment lacks objective criteria. Secondly, such an assessment would naturally be subject to considerable volatility, given that the actual value for the respective company may vary strongly, for instance depending on the concrete purpose and the applicable market conditions, especially for long-term contracts. Against this background, we believe the idea of disclosing to customers the economic value of data provided to the service provider – let alone have the customer participate in positive value developments – is impracticable. Instead, we recommend that more transparency regarding the use of data shall be provided, in order to enhance consumer data sovereignty.

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 adoption of DLT for specific applications, e.g. the storing and sharing of financial information, should be left to the market. At this stage it is not yet clear for which use cases DLT could offer significant benefits over alternative solutions. In accordance with the guiding principles for EU policies, as described in the introduction to this consultation paper, we recommend not to prematurely identify a potentially superior technical solution for a certain problem but rather leave it to the market.

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.

The European Commission seeks to facilitate the digital and cross-border use of electronic identification (and know-your-customer portability) on the basis of eIDAS, as laid down in the Consumer Financial Services Action Plan. We are however skeptical that the eIDAS framework is able to provide a sufficient solution for the private sector at least in the mid-term. Instead we advocate a more open market-driven regime with regard to the underlying technology.
A conceivable approach could be for instance a regime whereby banks could rely on past identifications provided by other banks. With such an approach, customers would only go through an identification procedure once at their bank ("as trusted party"); other banks or third party service providers should then be allowed to identify their customers by using the trusted party's data. This requires that the legal basis for error cases, and regarding liability issues, be developed.

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

Public ledgers can provide simple pseudonymous data storage, while private ledgers and interledger synchronisation provide more data protection. However, most problems regarding data security arise at the interface between the digital and the real world. Whilst not necessary within the system, a trusted partner is probably still needed at that point.

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?

Contrary to the assumptions here, there is only a slight advantage of data exchange in such cases. In the case of startups there is not much data available, so information systems and technology cannot provide better data for profiling.
Credit is given because the bank shares the same view on the possible revenues, and trusts the owner. This is similar to the case with an SME.

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?

The EBA has drafted guidelines for an ICT risk assessment for the financial sector, which were already taken up by the German banking authority as a national regulation. This regulation addresses all necessary aspects of ICT security management. Having a level playing field - and with this, having a common (cyber-)security level in Europe - is important. Therefore it would be necessary to establish a related implementation of the guidelines in the European Countries, and the requirements should be addressed to all financial service providers.
For proportionality it is important that the size, structure and operational environment of an institution are adequately taken into account when determining the scale and detail of the ICT 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?

Data privacy often is an issue when cyber-attacks are being traced and prosecuted. Finding the right measure to ensure an efficient prosecution while keeping personal data private is a difficult task, which needs an individual case-to-case consideration most of the time. Nevertheless, existing requirements should be addressed to all financial service providers.

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)?

Banks already have every possible test in place. As they are already strongly challenged by organised crime, talented individual hackers as well as security agencies, regulatory measures are unlikely to provide any additional benefits.

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?

```
The example of Bitcoin shows that technology-based innovations can
potentially avoid capture by regulation, even though they practically bypass
a highly regulated market. The regulator should ensure a level playing field
in all directions. Unnecessary entrance barriers should be avoided, while
necessary regulation needs to be enforced.
```

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:

6e8ac1b0-9607-41ad-a4d9-b0d265aad526/Full_Answer_3.1.docx

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