Brussels, 15 June 2017

THE EACB RESPONSE TO THE EUROPEAN COMMISSION CONSULTATION ON FINTECH: A MORE COMPETITIVE AND INNOVATIVE EUROPEAN FINANCIAL SECTOR

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Introduction

The European Association of Co-operative Banks (EACB) welcomes the opportunity to respond to the European Commission consultation on 'FinTech: a more competitive and innovative European financial sector'.

This document complements the responses given to the online questionnaire. We believe that not being able to motivate in the online questionnaire why you answer 'no'/'I don't know' to a given question, in our view risks delivering a bias towards 'yes' answer in the evaluation of the results of the consultation. We therefore elaborated justifications for questions where we answer 'no'/'I don't know' and we kindly ask the Commission to look at this document for those justifications.

General Comments

The definition of the word FinTech

As a general remark, the EACB is very supportive of the 'Digital Single Market Strategy for Europe'. We support and appreciate the following clarifications/definitions made in the consultation document:

- p. 4: ''FinTech' describes technology-enabled innovation in financial services, regardless of the nature or size of the provider of the services'.
- p. 4: 'The Commission's stance on FinTech relies on three core principles: technological neutrality, proportionality, and market integrity'.
- p. 16: 'Innovative firms, both start-ups and incumbents, can be subject to disproportionate, inconsistent or over-cautious application of regulatory requirements, as supervisors may lack the experience, expertise and guidance to respond to new developments'.

We welcome the alignment of these clarifications/definitions with the recent Financial Conduct Authority (FCA) discussion paper on Distributed Ledger Technology (DLT) launched in April 2017, notably [quote; p. 5]:

- 'Innovation can arise from diverse sources, such as start-ups, technology providers as well as regulated firms, including large financial institutions'.

This being said, we would like to submit that the term 'FinTech' is often used synonymously with 'FinTech start-up companies', thus ignoring that technology-enabled innovation in financial services does not depend on the size or legacy of a firm. Many banks, including co-operative banks, have been developing technology-enabled innovation in financial services for many years. In this respect, we urge the Commission not to fall into this overly simplistic equation.

FinTech versus access to financial services

Another point of imbalance stems from the 'digital divide' angle, that is, the fact that the adoption of FinTech banking facilities is concentrated among wealthier millennials, while older, less sophisticated and on average poorer consumers are left behind and only access banking through traditional channels. This may have particular relevance for co-operative banks as their traditional customer base may be skewed towards the digitally excluded. Linked to this, there is a risk that co-operative banks might be expected to continue serving this category at a high cost through branch banking (proximity) while the leaner, non-bank FinTechs have no corresponding obligation.

FinTech and regulation

Technology in and of itself is neither positive nor negative – social benefit will only accrue from how technology is used by both regulated and non-regulated market players. While the advent of the internet and web-related technologies has had the benefit of reducing transaction costs[1] for searching, evaluating and negotiating commercial relations, such efficiencies have also generated strong advantages for a handful of firms with huge economies of scale, resulting in nearly monopolistic structures[2] in parts of the e-business economy such as Amazon, Google, Facebook, Alibaba or Tencent.

All future developments are always uncertain and depend on 'trial and error' in the market. Regulation should be: (i) principle-based rather than rule-based; (ii) proportionate; (iii) consistent; (iv) balanced; (v) fully technology agnostic; and (vi) required only when justified by measurable data about any kind of misconduct or market misuse. Nonetheless, the principle 'same service, same risk, same rules' should apply.

We would like to also stress that:

- No new regulation is required at the moment, both because current legislation already addresses some aspects and because it's too early to define some other aspects that are still under development;
- If, however, regulation were to be undertaken, it should adhere strictly to previously indicated principles;
- Any regulation should ensure a level playing field that does not, on the one hand, hinder start-ups or, on the other, penalize financial institutions, especially smaller ones;
- Any positive measures aimed to foster FinTech (intended as technology-enabled innovation, as per the definition adopted by the Commission) at any level (funding, tax reduction, training, ideas sharing, etc.) are welcome as well as guidelines that could help to clarify or give examples of what can be done and how (as opposed to what cannot be done).

Co-operative banks, which are typically of smaller size and have close intimacy to their customers including SMEs, believe it is essential for regulation to be proportionate, balanced and capable of providing a level playing field without interference with the dynamic developments of a free market economy. One example can be taken from the various current developments in the field of data:

- Concerning personal data: the current EU General Data Protection Regulation (GDPR) and parts of the Payment System Directive 2 (PSD2) restrict the processing of personal data to contractual relations, mandates given by the customer, and/or explicit consent of the customer to the use of data by a data controller.
- In parallel Access to Accounts (XS2A) according to PSD2 and Portability of Data according to the GDPR (Art. 20[3]) open up contractual relations concerning data processing between a customer and her/his bank to third parties without a contractual relationship between the third party and the bank (as one side of the original contract).

[1] in the sense of the Transaction Cost Economies (TCE) of O.E. Williamson and other scholars.
[2] fully in line with textbook economics as at zero transaction costs only one monopolist should be able to survive.
[3] see the Article 29 Working Party Guidelines on the right to data portability.

- Finally, the Commission adopted the 'Building the European Data Economy' on 10 January 2017 with a focus on machine-generated data, but without clarifying how this fits with PSD2, as all customer data in a bank is processed by 'machines' (from mobile banking by smart phones to data centres).Nonetheless, no machine and no technology has a free will to enter into a contractual relationship. All existing technology – from printed paper starting in the 15th century in the modern form to leading-edge developments in 'artificial intelligence' – are used by people and are subject to existing civil and contractual law.

Collateral effects of technology

Technology can have collateral effects. For example, the idea behind Exchange Traded Funds (ETFs) is to invest in an 'index' provided by the market activities of all participants in equity trading in a certain segment. However, with robo-advice and ETFs one can imagine a world where most investments are made by such technologies, contradicting the original assumption of an 'independent' market with an index. Taking into account Eugene Fama's efficient market hypothesis, no investor can outperform an 'efficient' market, and, as a consequence no technology can provide better performance for a customer than market benchmarks in the long run.

This may be one illustrative example of technology providing more convenience for customers, but not better investment results in the end.

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, it could also create new barriers to access. In addition, 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?

Generally speaking, banks provide payment, banking/financial management tools (Web services, Apps and APIs) for their customers. Banks use technology-enabled innovation almost along 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

Please find below some examples from co-operative banks in Europe.

DZ BANK Group in Germany has used many (and maybe all) existing FinTech applications: from traditional COTS (commercial of the self) software such as SAP core banking via outsourcing and cloud-based services to applications provided by partners such as Business Process Outsourcing (BPO), Artificial Intelligence (AI), E-business payments (with e.g. iZettle and paydirekt), and blockchain/DLT (with e.g. Ripple).

As a financial institution providing a comprehensive range of services, the BPCE Group in France uses many existing FinTech solutions covering the different layers (back-end, middle, front-end and customer experience). It has developed partnerships with other FinTech firms/start-ups to provide better customer experience, security, quality, or to lower operational costs.

Gruppo Bancario Iccrea in Italy has been accelerating its involvement with FinTech applications; a new unit has been specifically created to follow and propose innovative digital initiatives. Among them, e-payments (Mybank), p2p payments (Satispay), Crowdsourcing, on line e-signature and webcam identification, big data (in partnership with Consorzio CBI) and other POC e.g. with Spid (e-IDs), blockchain for KYC or chatbots.

OP Financial Group (OP) provides multiple FinTech applications in its core business divisions for banking, non-life insurance and wealth management. Furthermore, OP is actively developing a new breed of services in its in-house accelerator programme and within its traditional core business lines. OP provides a mobile app for payments like P2P, online and NF-payments; mobile Point-of-Sale (POS); an easy-to-use personal finance management application showing consumption by different categories and predicting consumption in the future based on transaction data from the payment account; car loans evolved into Mobility-as-a-Service (MaaS); an invoicing and accounting platform for self-employed people and freelancers. In addition, OP is looking for ways to create new services to support new work economy and housing-related smarter services; mortgage loans supplemented with multiple third-party services (assisted house sale, moving services, cleaning, security and smart home IoT applications); smart health services integrated into insurance services; and, for insurance customers, a service guiding customers in the case of loss or damage.

With regard to the second part of this question, EACB members are mostly interested in new ways to define risk, provide loans (peer-to-peer and alternate lending), illustrate spending (PFM solutions of all sorts) and also new ways of identifying users, relaying trust (blockchain), doing payments and providing advice. We would also like to see more financial technology in the area of administrative services around money management, like APIs for tax or other e-government purposes that accept banks' identifications of customers to provide better overall services.

Further and more concrete RegTech solutions could be useful, if and when available, since compliance costs are still the most complex obstacles to freeing up the growth of innovative solutions.

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
X	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 yet.

Although 'automated financial advice' can produce a more reactive, real-time solutions to customers, for the time being, it remains is a niche technology. It is much too early to make any statistically significant measurements about the use of 'automated financial advice' today.

EACB members believe that the importance of automated financial advice will likely increase in the coming years. We see automated financial advice as an opportunity to enhance customer experience. Some customer groups, such as millennials, are likely more adaptive to new automated tools, whilst some customer groups might rely on personal advice. Roles of robo- and human-driven advice might also get blurred as human advice can be enhanced with efficient use of artificial intelligence.

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
X	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.

For the time being, 'artificial intelligence' is a niche technology. It is much too early to make any statistically significant measurements about the use of 'artificial intelligence' today.

We would like to stress that human reasoning should always be more valued than machine reasoning and reasonable exceptions to machine-generated decisions should always be implemented. For instance, a bank can be asked to give a customer credit, despite her/his history and AI analysis, because such customer is making a change in her/his life or profession and probably needs the credit to do so; this flexibility and ability to discern should guide banks' behaviour as well as regulatory requirements and oversight.

Financial service providers are already strongly regulated and supervised at EU and national level. When using algorithm or artificial intelligence applications, banks have to comply with all rules and regulation as if conducting business in a more traditional and manual way. Systems should be supervised and reviewed in conjunction with normal supervisory actions. It should be the duty

of the regulated entity, not the supervisor, to make sure that the use of algorithms or AI does not compromise market integrity or customer protection.

Regulation should not be technology-oriented but rather use-oriented.

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)?

In principle, 'automated financial advice' is 'financial advice' and is covered by MiFiD2/MiFiR. Any definition of customer segmentation is based on the customer profile and not on the technology used.

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?

In principle, 'automated financial advice' is 'financial advice' and consumer protection is covered by MiFiD2/MiFiR. Any definition of customer segmentation is based on the customer profile and not on the technology used. Additionally, the GDPR provides extra protection to the customer.

Having said that, 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 better identify a customer's personal situation, such as her/his risk appetite or temporary financial difficulties, as well as her/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 be recommended. This can support consumer and investor protection 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 prediction from Big Data is probably the best we have, but it is not perfect and cannot be exclusively relied upon for decisions.

We can in particular envisage two situations where Big Data prognosis reaches its limits:

- 'Black swans' (events so rare we do not yet have valuable statistical material); and/or
- Faults or biases in algorithms that cannot be detected within the regular (test) data or due to the learning aspect within 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 reasonable exceptions to machine-generated decisions should always be implemented.

Services should be upfront and open about the use of data and the benefits and risks associated. The creation of such services requires piloting and incremental development.

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
X	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.

For an overview, we would refer to the Cambridge Centre for Alternative Finance's 2016 European Alternative Finance Benchmarking Report (this report presents the research findings from the Annual European Alternative Finance Industry Survey in geographic Europe, which aims to systematically track and comprehensively benchmark the growth and development of the pan-European crowdfunding and peer-to-peer lending markets). For the time being, crowdfunding (in the sense of crowd lending) is a niche in continental Europe. Crowdfunding (in the narrower sense of donations to charitable initiatives) is already used by co-operative banks as the support of public-benefit initiatives is a part of the co-operative culture.

Crowdfunding might have many advantages, but it might also result in potentially high-risk investments. According to a comprehensive study of this sector, by AltFi Data and law firm Nabarro, one in five companies that raised money on equity crowdfunding platforms between 2011 and 2013 have since gone bust. As such, crowdfunding should be subject to the small investor protection law (e.g. the Kleinanlegerschutzgesetz in Germany). A recent study ('Praxiserfahrungen mit den Befreiungsvorschriften des Kleinanlegerschutzgesetzes' by the University of Trier, Humboldt-University of Berlin and ifo-Institute published in February/March 2017) commissioned by the German government came to the conclusion that one-third of crowdfunding volume has been used for property financing. As there already exist a broad variety of financial solutions in this financing segment, it is not necessary to have less strict financial regulation compared to property financing by banks.

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?

Imbalances and the lack of a level playing field concerning non-bank financing can create potential for regulatory arbitrage, with also a lack of clarity as to the contractual situation in peer-to-peer lending – who is lending to whom? Who is a principal, who is an agent? But this lack of clarity has not prevented the ballooning of P2P as savers scramble to find attractive returns, believing P2P investment is an alternative to protected bank savings. This creates serious potential for mishaps and damage to customers.

EACB members suggest that the MiFID II regime could be developed to include crowdfunding activities. This could be done over time on an evolutionary basis in the context of an ordinary review process.

On a practical level, we have noticed that there seem be diverging views on what regulated investment services (pursuant to MiFID II Annex 1, Section A) are provided and what the role of investment firms operating a crowdfunding platform is. There is a general agreement that firms operating a platform in most cases provide investment services such as '(1) Reception and transmission of orders in relation to one or more financial instruments'. However, there are diverging views as to whether or not the operation of crowdfunding platforms constitutes securities underwriting or Initial Public Offering (IPO) – types services regulated in Section A '(6) Underwriting of financial instruments and/or placing of financial instruments on a firm

commitment basis'; and '(7) Placing of financial instruments without a firm commitment basis'. The latter interpretation does not take into account the specificities of crowdfunding as a platform for smaller and mid-sized or start-up companies' fund raising.

This interpretation could hinder the development of MiFID-regulated crowdfunding platforms and should be further clarified by ESMA and/or the Commission.

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?

Any 'fund-raiser' or 'platform' is either a bank (with providing loans on their balance sheet) or a financial broker (as an interface between customer and bank). That should be the legal basis in the sense of a level playing field – especially with regard to customer protection.

Banks have a high level of transparency to customers for all the services they provide; any other provider of similar financial services should be regulated accordingly, also taking into consideration the risk for consumers; in particular, we suggest creating three levels of transparency (as for the financial sector):

- Precontractual;
- Contractual; and
- Post-contractual.

In some countries, there is new legislation on crowdfunding that stipulates statutory disclosure on fund-raisers. This disclosure regime is standardised and inspired by recent EU-level retail disclosure rules (Key Investor Information Document, PRIIPs and UCITS style).

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?

Insurance based on individual profiles and/or real-time monitoring of behaviour is a general challenge.

In principle, insurance is based on statistical probability, taking into account all insurance holders. Targeting individuals on an individual basis isn't 'insurance' in the traditional sense but individual risk mitigation. As such, it presents new risks and needs to be considered even beyond a regulatory context.

This being said, we believe that the challenges would be the following:

- Potential exclusion of certain consumers from certain services; even though we strongly believe that this challenge should be addressed more broadly than for the financial sector alone, considering that digitalisation itself might have an impact.

- There could be issues of incomparability of information arising, for example, where data relating to a customer but referring to different years is merged, potentially leading to situations where a customer could not receive a service or financial institutions could give credit where it shouldn't be given. We believe, however, that the market will solve these issues as more experience is gained with the use of sensor data analytics and other technologies. Should the market not be able to resolve this, guidelines or certification

mechanisms to standardise data sources, categories or other comparable metadata might have to be considered.

- There could be risks related to customer data quality and veracity, and it is necessary for financial services institutions to minimise such risks by way of proper processes, organisational set-up and control functions. It is also necessary to have in place a good complaint handling and monitoring process.

- Challenges linked to budget and human capital. Indeed, errors/inadequacies of sensor data analytics and other technologies are more likely to arise if tools are developed without the input of qualified staff. The need to ensure proper staff and the creation of new multidisciplinary teams with employees of different background is critical and is known. Experts having knowledge from both the data and business fields (holistic view) are demanded. Professional certifications (not only technical-statistical, but also business-related) should be developed and required when operating with sensor data analytics and other technologies.

Finally, we believe that the potential challenges described will only materialise where existing rules/legislation are not applied properly. The list of challenges is in a way already mitigated by regulations and not necessarily caused by sensor data analytics and other technologies. It is crucial for co-operative banks to have a more harmonised implementation of regulation across the European Union by authorities.

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

	yes
	no
X	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.)?

Insurance based on individual profiles and/or real-time monitoring of behaviour is a general challange.

In principle, insurance is based on statistical probability, taking into account all insurance holders. Targeting individuals on an individual basis isn't 'insurance' in the traditional sense but individual risk mitigation. As such, it presents new risks and needs to be considered even beyond a regulatory context.

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?

Technology has been improving the communication between customers and financial services providers for decades: from telephone banking starting in the 1980s via internet banking in the 1990s to banking apps and automated calculation based on 'artificial intelligence' today. This is market-driven development in a free market economy. Nevertheless, the activity of 'banking' itself is not dependent on technology and should thus also not be regulated based on technology but based on the activity or function performed. Any regulation should be (i) principle-based rather than rule-based: (ii) proportionate; (iii) consistent; (iv) balanced; (v) fully technology agnostic; and (vi) required only when justified by measurable data about any kind of misconduct or market misuse.

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?

Technology has been implemented in banks for decades, and efficiency improvement was always a driver in three major segments: (i) interaction/communication with clients (from paper to online); (ii) enhancement of interoperability by way of standardisation and common rules (incl. SWIFT and SEPA); and (iii) industrialisation/automation in operations. Collaboration has always been part of this development, from implementation of commercial software packages to collaboration between banks within the European Payment Council or at national level (e.g. the current 'paydirekt' solution in Germany) to cooperation with technology firms, from global players to start-ups.

The most promising use cases for FinTech are the automation of back-office processes, digital onboarding, digital customer service and blockchain efforts for sharing KYC data or other risk profiles.

Moreover, the use of web APIs should lead to more modular and flexible solutions which could improve processes and costs.

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?

We see a couple of measures, ideas, as follows:

- Key for such a market evolution would firstly be non-discriminatory access to technical or digital infrastructure components, because financial services depend more and more on these technical aspects:

  - messaging services need to be designed with the following characteristics:
    - pseudonymous address book matching;
    - sufficient encryption to protect privacy of financial facts; and
    - non-discriminatory access for enterprise use.
  - Wireless features such as NFC or fingerprint scanners, system integrity and advanced (passive) authentication processes.

- Customer protection will be equally important. Markets need to evolve in such a way that the trust of customers is always ensured. A level playing field needs to be implemented taking into account risk adjustments and full risk transparency for the customer.

- A liability/responsibility framework needs to be put in place that allows putting the responsibility towards clients with the party that performs the service, unless otherwise agreed by contract. Should consumer protection necessitate that the burden of this responsibility is put upon another party then the liability framework should allow contracts between the two parties concerned to manage this delegated responsibility.

  Some ideas from outside Europe work around things like specific development programmes to finance experimentations (e.g. with fiscal exemptions), the creation of sandboxes to freely test innovations, encourage ideas sharing, production and execution, promoting acknowledgement, diffusion and training on such topics by facilitating cooperation between universities, financial institutions, talent gardens, customer associations and other stakeholders.

- With regard to cloud computing, we think there should be a common understanding at EU level as to how to safely use cloud computing in the financial sector. This would remove barriers and obstacles that financial institution are facing in using cloud computing. Cloud providers should be encouraged to develop cloud infrastructure that is accepted by financial supervisors and suitable for financial institutions.

- On blockchain technology in the field of securities markets, we would like to refer to a recent ESMA report on 'The Distributed Ledger Technology Applied to Securities Markets'. We agree that the current EU regulatory framework does not represent an obstacle to the emergence of DLT in the short term and new solutions should comply with the existing regulatory framework. However, in more detailed questions there would be room for further elaboration and reflection on how EU rules (such as the Financial Collateral Directive, the Settlement Finality Directive, etc.) are applied to new digital assets such as 'cryptosecurities'.

We are firmly convinced that no specific regulations are needed at EU level. If at all, any regulation should be: (i) principle-based rather than rule-based; (ii) proportionate; (iii) consistent; (iv) balanced; (v) fully technology agnostic; and (vi) required only when justified by measurable data about any kind of misconduct or market misuse. Nonetheless, the principle 'same service, same risk, same rules' should apply.

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?

A brand-new field of needs and correlated skills is rapidly growing. New job opportunities in many sectors can be invented, too. Therefore, new competences have to be developed and encouraged. These competences have to be a mix of technological, business, banking and user experience ideas and, more difficult to find and obtain, a continuous focus on new ways of thinking, new

ideas and new solutions to satisfy new and fragmented customer needs and to bring concrete value to real-life problems in a more complex world.

These competences change fast, due to fast emerging innovations, so it is really difficult for traditional HR units to follow, and sometimes understand or anticipate, trends and needs.

We would like to point out that technology cannot replace all employees. There is still a need for human skills in different tasks. Human labour is necessary in training and more complex operations. Even though machines and AI can also be used for customer service, more complicated and demanding customer service will not be replaced by machines.

Digitalisation is already the new industrial revolution, so it is not sufficient anymore to be a simple digital native: attitudes must be correctly addressed, encouraged, supported and trained with suitable initiatives since early school and then with extensive education programmes, sharing of experiences at European (or worldwide) level. Therefore, financing and promoting programmes in this direction is welcome.

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 term RegTech is a marketing term without much content. Banks have been implementing technology for compliance purposes (e.g. for statuary reporting) for decades. Proportionality is the key issue for co-operative banks, as small local co-operative banks are forced to comply with rules designed for international investment banks.

Should further and more concrete RegTech solutions become available, they could be useful as compliance costs are still the most complex obstacles to freeing up the growth of innovative solutions. For example, automated testing, availability analysis and other methods could be used by regulators to secure availability and trust in publicly available services without interfering daily routines within banks.

But RegTechs alone are not sufficient. Concrete initiatives to facilitate innovation without too many burdens are to be put in place by the EU.

No new rules are required but positive measures, deregulation in certain ‘safe’ areas as well as financing or facilitating economic support to create simple compliance frameworks or examples to follow.

These measures should be the same for start-ups and for traditional financial institutions so as to guarantee a level playing field.

With regard to challenges, these include among other things cyber risks, data security issues and other technology-related risks. In order to mitigate such risks there should be more international collaboration between the public and private sectors as well as common policies and practices.

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

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

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

As a general comment, EACB members support the European Commission's steps to remove obstacles to the free movement of data, as stated in the Communication on 'Building a European Data Economy' adopted on 10 January this year. In particular, we support the Commission's intention to enter into structured dialogues with the Member States and other stakeholders and, following such dialogue, possibly launch infringement proceedings to address unjustified or disproportionate data location measures as well as further initiatives on the free flow of data.

Moreover, whether it is 'cloud', 'outsourcing', 'hosting' or 'on premise', banks have to comply with data security regulations in Europe. The reasons to use a given operational model are based on commercial calculations. For example, our German member uses all four models in a hybrid approach for running its IT systems.

One specific example is the use of SWIFT by banks for messaging services, with SWIFT storing message data (which may contain personal data) in multiple operating centres for resilience, availability and security purposes in the EU and in the US. Therefore, the European Commission's initiative to launch the 'EU-U.S. Privacy Shield' (July 12, 2016) for stronger protection for transatlantic data flows was highly appreciated.

In some Member States cloud computing is not so often used by financial institutions due to the rather negative attitudes of supervisors. For instance, the Finnish FSA has in its current practice limited the use of cloud computing due to security concerns. This prevents financial institutions from benefitting from storing and processing data in multiple locations within the EU and benefitting from cost savings.

As said under question 2.2, we think there should be a common understanding at EU level as to how to safely use could computing in the financial sector. Cloud providers should be encouraged to develop cloud infrastructure that is accepted by financial supervisors and suitable for financial institutions.

Question 2.5.2: Does this warrant measures at EU level?

	yes
	no
X	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.

n.a.

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

X	yes
	no
	Don't know/no opinion/not relevant

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

Banks decide their IT operational models based on evolution of costs, quality, security and capabilities.

Depending on the kind of cloud solution offered, providers could facilitate adoption by banks through a sort of 'standard legend' based on icons or compliance tables (reflecting contracts) like Common Criteria for copyright. In this way, buyers could immediately and easily know if a provider is GDPR or PCI-DSS compliant.

The EU could help providers in creating and updating these schemes.

No regulatory measured are required for the time being.

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

	yes
X	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.

Banks decide their IT operational models based on evolution of costs, quality, security and capabilities.

No extra regulation is required. Importantly, contracts should comply with the GDPR.

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?

DLT offers new opportunities in any sector that needs or wants to offer more transparency, traceability, and community building (peer-to-peer exchange). Advantages include fewer intermediaries and the ability for investors to face borrowers more directly (cost reduction, more transparency), leading to direct investment/better access to financing and new market opportunities due to process simplification. DLT also has the potential to expand the range of potential opportunities for investors as permissionless blockchains could offer a ready-to-use decentralised notary service operated by user.

DLT is not just a technology but a new paradigm. Its founding principles (peer-to-peer exchange without central authority, access to all and transparency…) have opened up a wider field of study, notably as relates to the digitalisation of all processes with many actors (among which customers and especially SMEs).

This digitalisation could be applied to various uses in the banking industry, with benefits in term of costs and new opportunities. DLT could allow cost efficiencies for SME financing by enabling interoperability amongst various parties to the transaction (sharing of data, etc.). Any cost

savings in the process can improve access. The use of 'smart contracts' could also be envisaged to improve contract execution.

However, DLT is also at a very pre-mature stage and its use holds several challenges (see also the ECB's special report 'Technological innovation: Distributed Ledger Technology (DLT) – challenges and opportunities for financial market infrastructures'). We would thus, at this stage, prefer not to make any recommendations in the context of this question.

As DLT is a general-purpose technology (comparable with other data base management systems), it is not client-specific.

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)?

Challenges and a (first) risk assessment of DLT are discussed in a recently paper by Milkau et al. ('Development of distributed ledger technology and a first operational risk assessment', Capco Journal of Financial Transformation, Vol. 44, 2016). We would like to refer to this publication and mention only one specific challenge.

Box 1 on page 12 of the EC consultation document says that: 'DLT has the potential to disintermediate and automate processes, reducing counterparty and operational risk'. This can be taken as an example for misunderstanding the potential of DLT and technology in general. While DLT can reduce settlement risk – similar to Continuous Link Settlement – due to a synchronisation of the two legs of a transaction, a counterparty risk is always linked to a potential default of the counterparty in the future, which depends on the financial condition of a firm, but not on the technology underlying a message exchange. Therefore misunderstanding may be the largest danger in the current discussion about DLT (and about any FinTech in general).

Additionally, the original version of DLT as implemented e.g. with 'Bitcoin' or Ethereum was a so called 'permissionless blockchain', which works in an open peer-to-peer computer network. Nevertheless, for the synchronisation of all notes to store the same data 'on the blockchain' a special consensus mechanism is needed, which is by definition very resource-consuming and highly inefficient.

The technology component is still moving given the many communities that enrich each other. Interoperability is still a subject that is little discussed and which generates uncertainties for a possible long-term choice. We expect several DLTs to coexist in the long run, so interoperability will be key.

Several challenges remain for an implementation involving lots of clients:

- Appropriation by the customer of this new trust approach.
- Liability management to be defined.
- Governance:
  - of the underlying blockchain for public blockchains
  - of the consortium for permissioned blockchains
  - of the systems issue
- Integration in the internal banking ecosystem: each business line must identify the disruption of its approaches.

As currently all DLT implementations are proprietary solution without interoperability due to missing standards, DLT is not mature for a large-scale implementation and/or for systemically critical financial infrastructures.

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?

As a technology for messaging and data storage, DLT does not require any special treatment. Already today, electronic communication systems are used to exchange messages within contractual relations (from SEPA payments to confirmation of derivate financial instruments). As 'Smart Contracts' are simply computer code or 'scripts', they do not require any extension of existing law, which already covers electronic communication as part of contractual agreements.

Nevertheless, contract laws are different across Europe and even more so internationally. Therefore, harmonisation of European law – e.g. in the case of the planned Securities Law Legislation – is appreciated.

As the banking services to which this technology could be applied are not clearly defined, the potential obstacles are difficult to identify at this stage. However, among topics warranting specific attention, we would like to mention enforceability of the smart contract and of the digitalisation of documents. In its report ESMA 'believes that it is premature to fully appreciate the changes that the technology could bring and the regulatory response that may be needed, given that the technology is still evolving and practical applications are limited both in number and scope'.

Given the capabilities of the technology, we expect regulators to open up the possibility of it being used for functions traditionally held by some actors (e.g. Central Securities Depository could be replaced by DLT-based systems).

Nevertheless, when laws are not technologically neutral it could be necessary to revise them in order to erase this lack of neutrality.

It is particularly important to design blockchains that respect the regulatory framework on data and privacy.

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
X	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.

Generally speaking, taxes (especially VAT) provide a big hurdle to outsourcing. Outsourcing – in various types, from pure data centre outsourcing to business process outsourcing – is quite common to banking and financial services.

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

X	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.

For outsourcing and the so-called 'outsourcing risk', there are regulatory requirements at European (e.g. Supervisory Review and Evaluation Process (SREP)) and national level (e.g. 'MaRisk' in Germany). In such regulations the roles and responsibilities of banks and outsourcing providers are defined. However 'outsourcing' per se does not generate a risk, but is part of the risk management of every bank concerning operational risk and IT security.

We would like to comment though that PSD2 in a way is contradicting the presently existing outsourcing requirements. Indeed, the concept of third parties initiating payments for bank clients could be seen as a bank functionality being outsourced to a third party. Under the outsourcing rules banks should conclude contracts with such parties to manage the risk transfer. However, PSD2 does not allow banks to ask for such contracts.

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?

There are many technological developments with potential for increased efficiency: from personal assistants such as Siri or Alexa to Robotic Process Automation. Biometrics including 'behavioural biometrics' (specific movement, typing pattern) have large potential for strong and customer-friendly authentication. All those technological developments are market-driven and will be implemented if banks see benefit in doing so.

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?

As all regulation should be technology neutral, no regulation of technological innovations is needed, as long as different regulations are consistent.

But certain inconsistencies do exist. Let's look at various current developments in the field of data:

- Concerning personal data: the current EU GDPR and parts of PSD2 restrict the processing of personal data to contractual relations, mandates given by the customer, and/or explicit consent of the customer to the use of data by a data controller.

  In parallel Access to Accounts (XS2A) according to PDS2 and Portability of Data according to the GDPR Art. 20 (see also the Article 29 Working Party guidelines on the right to data portability) open up contractual relations concerning data processing between a customer and her/his bank to third parties without a contractual relationship between the third party and the bank (as one side of the original contract).
- Finally, the Commission adopted the 'Building the European Data Economy' on 10 January 2017 with a focus on machine-generated data, but without clarifying how this fits with PSD 2 as all customer data in a bank is processed by 'machines' (from mobile banking by smart phones to data centres).

Synchronisation can be done during consultation and discussion of new initiatives.

In general, it could be easier to issue Regulations and not Directives to have a competitive market. In the interim period, given the present regulatory framework, guidelines such as those provided by the WP29 can be a good approach to provide rules that allow FinTech to act within the same provisions.

Another important aspect is that different sectorial legislation states that service providers must give customers pre-contractual information usually with a certain information sheet. Service provider typically provide such information in paper form. It is difficult to implement such requirements on websites and mobile channels because it is usually forbidden to make any changes to these pre-defined information sheets. Some examples that exist in current legislation are the following:

- European Standardised Information Sheet (ESIS) relating to mortgage and consumer loans;
- Packaged Retail Investment and Insurance Products (PRIIPs): Key Information Document (KID);
- Insurance Distribution Directive (IDD): Insurance Product Information Document (IPID);
- Pre-contractual information relating to payment services; and
- Pre- and post-information of prices relating to prices of basic payment accounts.

Service providers should be able to provide the required information in a way that is suitable to the multiple channels currently available.

Finally, as said under question 2.2, in some Member States cloud computing is not so often used by financial institutions due to the rather negative attitudes of supervisors. For instance, the Finnish FSA has in its current practice limited the use of cloud computing due to security concerns. This prevents financial institutions from benefitting from storing and processing data in multiple locations within EU and benefitting from cost savings.

We think there should be a common understanding at EU level as to how to safely use could computing in the financial sector. Cloud providers should be encouraged to develop cloud infrastructure that is accepted by financial supervisors and suitable for financial institutions.

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

The most efficient path for any innovation is market-driven development. Therefore, any active regulation should be: (i) principle-based rather than rule-based; (ii) proportionate; (iii) consistent; (iv) balanced; (v) fully technology agnostic; and (vi) required only when justified by measurable data about any kind of misconduct or market misuse.

The Commission should always apply the principle of 'same activities, same rules and same supervision'.

Regulation addressing the access to infrastructure needs to allow new participants to enter the market, whilst at the same time allowing infrastructure providers to have sufficient returns and business model flexibility to upgrade and evolve the infrastructure.

Essential infrastructures for mobile payments need to be accessible to all players in the market and not limited to mobile device manufacturers. The regulator should ensure that all payments service providers are able to access the technology components, e.g. for authentication (e.g. fingerprint scanner) or data transmission (e.g. NFC, Bluetooth Low Energy), that are required for M-Payment solutions.

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
X	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?

This is a difficult question. Some very limited action is necessary as follows:

- Establishment of a liability/responsibility framework that allows putting responsibilities towards the customer with the institution that performs the service unless otherwise agreed by contract;
- Establishment of a technology neutral level playing field through compliance monitoring;
- Monitoring of further market evolution to ensure that:
    - No new forms of financial exclusion develop as a result of (intended or unintended) cherry picking by new FinTech solutions/providers;
    - A sufficiently rich and diverse landscape of financial services providers remains (both in terms of company size as in terms of company type (shareholder versus stakeholder models).

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.

As stated on page 4 of the EC consultation: 'FinTech' describes technology-enabled innovation in financial services, regardless of the nature or size of the provider of the services.'

Therefore, question 3.3 is unclear – FinTech can be used regardless of the nature or size of the provider of the services. Care should be taken in evaluating this question and not to mix the concept of FinTech with that of Start-up. Large, existing companies can also be defined as FinTech.

Moreover, the EU Financial Services acquis already provides efficient tools for FinTech firms (as per the definition adopted by the Commission) to scale up. The EU level passport provides access to EU27 markets and guarantees high levels of consumer protection and market integrity concurrently. There is no need to create a separate regulatory regime for start-up companies. The principle 'same service, same risks, same rules' should apply. As we have indicated elsewhere, even smaller start-ups have been able to obtain licences as investment firms and scale-up their crowdfunding business.

Concerning licensing requirements, the existing legislation and regulation define what a 'bank' or a 'payment institute' are. Any kind of 'shadow banking' contradicts the approach of a level playing field.

On page 8 the consultation paper says: 'Non-bank financing, including peer-to-peer/marketplace lending, reward and investment (or equity) crowdfunding, as well as e-commerce finance, invoice and supply chain finance platforms, is offering new channels of access to finance for individuals and small companies facing difficulties to tap the traditional banking channels, especially due to the lack of appropriate collateral or provide historical credit information (e.g. low income borrowers or start-ups).'

As co-operative banks have been traditional banking channels to members, clients and SMEs, any 'non-bank licensing' for lending or other financial services distort the level playing field, including the risk of a new kind of 'sub-prime crisis', and would weaken those banks which are sustainable pillars of the economy.

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
X	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 believe that there is no need to introduce new licensing categories as licensing categories should be technology neutral. New licensing categories can only be provided for new services. We currently see no such services. And once again, the principle 'same service, same risks, same rules' should apply.

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?

X	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.

Small and local co-operative banks especially suffer from regulatory burdens, e.g. reporting requirements, which are designed for large and/or international banks but do not fit to the nature of co-operative banks playing a major role in the financial and economic system. Co-operative banks contribute widely to stability thanks to their anti-cyclical behaviour; they are the driver of local and social growth with 4,050 locally operating banks and 58,000 outlets; they serve 210 million customers, mainly consumers, SMEs and communities. In supporting more proportionality, therefore, the Commission should look at the entire financial services value chain and not focus on non-bank FinTechs specifically.

The Commission should always apply the principle of 'same activities, same rules and same supervision'.

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?

X	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.

In our view, 'free flow of data in the Digital Single Market' means applying the principles of a free market economy and freedom of contract to the issue of data provided and/or processed in a contractual relationship between a client and a financial institution. Banks have always been a custodian of their clients' data and processed such data in a contractual context. This can include checks for AML/CTF in payments or credit scoring in loans and mortgages as legitimate parts of processing in the context of a contractual relationship.

For international (cross-border) transactions – such as payments, trade finance, securities settlement, etc. – it is, of course, condition sine qua non that transaction messages can flow freely, but this flow is defined in the contract between a customer and her/his bank.

Nevertheless, with the PSD2 the freedom of contract, including the right of an entity not to enter into a relationship with a third party, has been restricted. Therefore, an asymmetric situation will be enforced by regulation (i.e. PSD2), as customers have to give their consent to a third party, but banks must not.

In our opinion, it will be a key success factor for the Digital Single Market to be based on the fundamental principles of market economy and basic features of contract law. Any restriction of these general principles which single out a particular context to enforce a single rule concerning access to data will undermine the basis of the Single Market.

Moreover, due to legacy IT systems in conventional banks, new players like start-ups are often in a better position to implement a 'free flow of data'. There must be a level playing field in the use of customer data by start-ups, banks and other market participants. As an illustration, it should be noted that the PSD2 will not allow reciprocity of access to information between credit institutions and the new categories of service providers.

It is also worth mentioning that in some countries (e.g. Austria, Finland, France, Germany) there are some restrictions relating to use of payment data for credit institutions. For instance, restrictions in the Finnish Credit Institutions Act limit the use of payment data for marketing purposes and the sharing of data within a group.

Finally, in some cases strict EU data protection provisions (e.g. the right to object to decisions based on profiling) could act as a competitive disadvantage for European innovation vis-à-vis firms operating and serving customers in other regions of the world. European competitiveness should not be forgotten.

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

X	yes
	no
	Don't know/no opinion/not relevant

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

Yes. With regard to proportionality, however, the principle of 'same business, same risks, same rules' must not be compromised. To complement the three principles, subsidiarity in regulation in general and customer protections should be added as fourth and fifth guiding principles.

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?

As any regulation should be technological neutral, the Commission and European Supervisory Authorities should coordinate a common understanding that 'technology' should not be regulated but left to the market to develop market-driven innovations. The more the Digital Single Market will be based on the fundamental principles of market economy and basis features of contract law, the more market-driven innovations have the potential to develop.

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

X	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.

The ESAs should understand technological developments. Financial services are based on technology to a high degree, and data protection, IT security and cyber resilience are key for the stability of the financial system in Europe and globally.

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

X	yes
	no
	Don't know/no opinion/not relevant

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

It is essential for the Digital Single Market's success for all stakeholders of the financial systems to have a clear and common understanding of what technologies can do (and not do), what principles of the market economy have to be strengthened and when – as a last resort – regulation might be needed. A 'European Innovation Platform' as a common hub for discussion and support of a strong European economy can be helpful, but should not interfere with existing European initiatives. Moreover, such academy should remain limited to the sharing of knowledge and best practices. It should not endeavor in defining recommendations for action unless its composition is sufficiently representative of the wide European stakeholders in this debate.

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

	yes
X	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?

Although not against sandboxes, we are not convinced that sandboxes can provide better results compared to market-driven innovation. If any guidelines or regulation are to be contemplated, such guidelines/regulation should take care to focus sandboxes or other FinTech facilitators both on new (start-up) and incumbent (e.g. banks) FinTech providers and ensure a level playing field with those outside the sandbox by ensuring transparency on the experiments going on and any regulatory 'lenience' considered.

More in general, we would like to also stress that:

- No new regulation is required at the moment, both because current legislation already addresses some aspects and because it's too early to define some other aspects that are still under development;
- If, however, regulation were to be undertaken, it should adhere strictly to previously indicated principles, especially 'same service, same risks, same rules';
- Any regulation should ensure a level playing field that does not, on the one hand, hinder start-ups or, on the other, penalize financial institutions, especially smaller ones;
- Any positive measures aimed to foster FinTech (intended as technology-enabled innovation, as per the definition adopted by the Commission) at any level (funding, tax reduction, training, ideas sharing, etc.) are welcome as well as guidelines that could help to clarify or give examples of what can be done and how (as opposed to what cannot be done).

As all players in the European financial system are competing in the global economy with major international banks and internet juggernauts – such as Google, Amazon, Alibala, Tencent, etc. – any limitation to the competitiveness of European banks, including co-operative banks, should be avoided.

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

	yes
X	no
	Don't know/no opinion/not relevant

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

Although not against sandboxes, we are not convinced that sandboxes can provide better results compared to market-driven innovation. If any guidelines or regulation are to be contemplated,

such guidelines/regulation should take care to focus sandboxes or other FinTech facilitators both on new (start-up) and incumbent (e.g. banks) FinTech providers and ensure a level playing field with those outside the sandbox by ensuring transparency on the experiments going on and any regulatory 'lenience' considered.

More in general, we would like to also stress that:

- No new regulation is required at the moment, both because current legislation already addresses some aspects and because it's too early to define some other aspects that are still under development;
- If, however, regulation were to be undertaken, it should adhere strictly to previously indicated principles;
- Any regulation should ensure a level playing field that does not, on the one hand, hinder start-ups or, on the other, penalize financial institutions, especially smaller ones;
- Any positive measures aimed to foster FinTech (intended as technology-enabled innovation, as per the definition adopted by the Commission) at any level (funding, tax reduction, training, ideas sharing, etc.) are welcome as well as guidelines that could help to clarify or give examples of what can be done and how (as opposed to what cannot be done).

As all players in the European financial system are competing in the global economy with major international banks and internet juggernauts – such as Google, Amazon, Alibala, Tencent, etc. – any limitation for the competitiveness of European banks, including co-operative banks, should be avoided.

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

For any kind of market-driven innovations, a level playing field is a key success factor. If needed, any regulatory measured should be: (i) principle-based rather than rule-based; (ii) proportionate; (iii) consistent; (iv) balanced; (v) fully technology agnostic; and (vi) required only when justified by measurable data about any kind of misconduct or market misuse. Nonetheless, the principle 'same service, same risk, same rules' should apply.

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?

X	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.

The consultation paper raises a number of interesting points regarding standards and interoperability. With regard to the question whether they are sufficiently addressed, we would like to point out the following:

- When it comes to technology, Europe and the financial industry in Europe can not be seen as isolated from the rest of the world;
- At international level, several well governed standardisation bodies – such as ISO 20022 – exist. With the implementation of SEPA on the basis of XML and ISO 20022, a great success was achieved for the current and future interoperability in the European payment system. At European level, also different standardisation initiatives exist;
- Whilst participation to standard setting initiatives should be unrestricted and procedures for the adoption of standards transparent, it should also be recognised that too many parties around a standardisation table will slow down the standardisation process keeping interested firms from moving forward;
- Fragmentation can indeed impair market efficiency but an initially fragmented standards development by a few parties that is followed by work on interoperability by those same parties may deliver faster integration then an all inclusive standardisation work; and
- Technical standards should not be regulated but should be market-led.

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

	yes
X	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.

We do not see the link between standardisation and outsourcing as it is portrayed in this question.

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?

As observed for question 3.12.1, ISO 20022 is a good example for international standardisation driven by industry developments. Taking this into account, a free market-driven development is the best way to achieve interoperability – especially in an interconnected network market such as financial services.

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
X	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.

International standardisation processes are working very well. For blockchain technologies, the ISO/TC 307 international technical committee for the development of blockchain standards was recently set up. The committee also involves 16 ISO member bodies, including Germany, the United Kingdom, France, Estonia, Canada, Australia, the United States, Japan and South Korea.

No measures at EU level are needed to promote the use of technology, including open source.

The development of open source model libraries should be market-driven and based on freedom of contract.

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.

In the introduction to question 3.15 two statements are made, which are unclear:

1. '[...] and the arrival of FinTech firms [...]' (page 18 of the EC consultation document).

➔ As elaborated before, page 4 of the Consultation document explains that ''FinTech' describes technology-enabled innovation in financial services, regardless of the nature or size of the provider of the services'. Therefore, 'FinTech firms' is a contradictio in adiecto.

2. 'It is important that supervisors closely monitor the adaptation process of incumbents to new technologies' (page 19 of the EC consultation document').

➔ As page 4 also says 'The Commission's stance on FinTech relies on three core principles: technological neutrality, proportionality, and market integrity', it is fully unclear why supervisors should monitor the adaption of any kind of technologies, and why they should monitor incumbents only.

Financial technology can bring different kinds of efficiencies to institutions (both incumbents and new companies). Indeed, it is the reason why banks have not stopped introducing new kinds of technology into its daily service offer over the last 30 years (technology enable electronic payments!). In todays world, new financial technology brings efficiencies in for example the communication with customers (more user friendly channels, formats, colour schemes, control modules etc.), back office functions (e.g. DLT), ways to store and analyse customer data and speed of execution of transactions. Some of these technologies, but perhaps more so the companies that are (allowed or not) using them to compete with incumbents, do however also create risk and thus have an impact of the safety and soundness of incumbent firms. This is the case where such technology leads to additional operational risk such as when:

- Incumbent firms are positioned as infrastructures for other providers to benefit from without financial compensation for the use of these infrastructures;
- The financial technology leads to multi party financial ecosystem without a clear contractual framework that determines, between the different parties, who takes

responsibility towards the customer and how to further deal with compensation between the parties;
- The introduction of such technology creates increased chances of cybercrime.

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 our view, 'free flow of data in the Digital Single Market' means applying the principles of a free market economy and freedom of contract to the issue of data provided and/or processed in a contractual relationship between a client and a financial institution. Banks have always been a custodian of their clients' data and processed such data in a contractual context. This can include checks for AML/CTF in payments or credit scoring in loans and mortgages as legitimate parts of processing in the context of a contractual relationship.

For international (cross-border) transactions – such as payments, trade finance, securities settlement, etc. – it is, of course, condition sine qua non that transaction messages can flow freely, but this flow is defined in the contract between a customer and her/his bank.

Nevertheless, with the PSD2 the freedom of contract, including the right of an entity not to enter into a relationship with a third party, has been restricted. Therefore, an asymmetric situation will be enforced by regulation (i.e. PSD2), as customers have to give their consent to a third party, but banks must not.

In our opinion, it will be a key success factor for the Digital Single Market to be based on the fundamental principles of market economy and basic features of contract law. Any restriction of these general principles to enforce a single rule concerning access to data will undermine the basis of the Single Market.

The second part of this question is unclear as the GDPR explicitly requires the data subject's consent for a service provider (data controller) to process the data for specific use.

In our view there is an inconsistency of the proposition of 'fair compensation' with the philosophy of the GDPR. As an illustration it must be underlined that the data subject has the right to withdraw her/his consent at any time. Thus, the data subject could receive the fair compensation and then withdraw her/his consent.

Having said that, we believe that any further commercial purpose should be made clear to the customer.

From the point of view of a free market economy and of freedom of contract, the statement on page 20 'big companies holding large amounts of data do not give data access to other businesses' sounds strange, as nobody would expect from a large retailer – including e.g. Amazon – to give access to its internal data (based on the contractual relationship with its clients).

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 use of the DLT can improve the auditability and reliability of data.

Data is key in the financial sector (KYC, transaction data, reference data, market data, etc.). The implementation of DLT solutions requires data standardisation that can provide some added value to the sector.

For quite some time, distributed databases (and DLT) have provided the advantage of storing data at multiple locations in a network and avoiding the danger of a 'single point of failure'.

DLT solutions allowing the creation of decentralised networks are particularly interesting for information storing and sharing in co-operative groups, which are decentralised and composed of many entities.

However, this comes with a price as this redundancy requires dedicated protocols for synchronisation (such as consent mechanisms in DLT). Regardless of this technical balance between availability and required resources, the question of governance remains, i.e. which entities run those distributed databases?

In the case of 'Bitcoin' the original peer-to-peer approach collapsed over time and today a limited number of opaque and interlinked 'mining pools' are in control of the majority of resources and data storage. Additionally, 'permissionless blockchain' as used by Bitcoin or Ethereum stores all data in clear readable format, and everybody is able to retrieve and read all stored data.

Current developments such as Ripple's InterLedger Protocoll or R3's Corda framework implement 'permissioned' versions of DLT within closed groups of identified users (such as banks) and can limit access to defined parties. Also, some of these new protocols offer the possibility to encrypt transaction data, allowing for a strict confidentiality of the transactions between parties. These developments can be seen as advanced protocols for synchronisation of (existing) ledgers inside different financial service providers without the need for later reconciliation and without separation of clearing (of messages) and settlement (of funds). These market-driven developments offer some promise to overcome the limitations and inefficiencies of the original DLT, but are still at a very preliminary stage and are not interoperable for the time being.

As DLT is a toolbox with a number of long-existing single technological building blocks, a market-driven development and selection of commercially useful technology solutions have to provide more insight about costs and benefits of this technology in the future.

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

	yes
X	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.

As answered under question 4.2, 'permissionless blockchain' as used by Bitcoin or Ethereum stores all data in clear readable format, and everybody is able to retrieve and read all stored data. The 'identity' of the user or, more correctly, the person with the right to claim the token within an existing transaction is given by a cryptographic public/private key pair (i.e. pseudo-anonymity), but not by an existing digital identity framework.

However, with developments such as Ripple's InterLedger Protocoll or R3's Corda framework, the implementation of 'permissioned' versions of DLT within closed groups of identified users (such as banks) can be enhanced by existing digital identity frameworks. This requires more development work in the future.

This being said, there is currently no real e-identity available for customer registration (retail or corporate) and digital identity frameworks are not sufficiently developed.

In parallel, some proposals have been made to use DLT itself for digital identity management (e.g. by the companies 'Blockchain Helix', 'FranceConnect'). Although those proposals seem to have benefit e.g. for KYC, none of them is at a mature stage today.

As a last remark, it should be noted that in all solutions for financial market infrastructures a unique identification of the (direct) counterparties such as a BIC or a LEI is an essential standard for global use. This standardisation is completely outside the scope of DLT although some DLT-related working groups are studying the subject.

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

As answered under question 4.2, 'permissionless blockchain' as used by Bitcoin or Ethereum stores all data in clear readable format, and everybody is able to retrieve and read all stored data. Current developments such as Ripple's InterLedger Protocoll or R3's Corda framework implement 'permissioned' versions of DLT within closed groups of identified users (such as banks) and can limit access to defined parties.

Also, some of these new protocols offer the possibility to encrypt transaction data, allowing for a strict confidentiality of the transactions between parties.

It could be interesting to further explore the potential of using DLT to store and share informational on KYC-AML. There are already some FinTechs (e.g. Tradle) offering this service through DLT. But implications with personal data protection still have to be better understood due to the nature of DLT itself, e.g. the fact the data is in a clear and readable format or how to comply with the 'right to be forgotten' required by GDPR.

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?

Before answering question 4.5, three remarks have to be made concerning the introduction to this question:

1. It is unclear what 'Non-bank funding providers' are (page 21 of the consultation document). Either a lender takes a loan on its balance sheet – in which case this is a banking business and requires a banking licence – or a financial broker acts as an interface between a borrower and a creditor. As it can be seen with the example of 'marketplace

lending', the original idea of 'person-to-person crowdlending' developed very fast into the current marketplace lending with a typical process chain from a borrower to match-making portals to bank and financial investors (bank or often shadow-banking entity).

2. Co-operative banks play in particular a major role in the financial and economic system as they contribute widely to stability thanks to their anti-cyclical behaviour. They are the driver of local and social growth with 4,050 locally operating banks and 58,000 outlets; they serve 210 million customers, mainly consumers, SMEs and communities. Typically, they provide loans to SME and in many cases across Europe. Co-operative banks have increased lending in recent years.

3. It is unclear what kind of 'information asymmetry is a barrier to SME's access to finance' (page 21 of the consultation document). Usually an SME applying for a loan provides all required information to a bank and the bank itself uses its credit risk scoring and management systems (as required by the regulation for credit risk management in banking).

As risk profiling is a core competency of banks – and in particular of banks serving SMEs such as co-operative banks – technology for scoring and credit risk management has been used for many years. Especially in the SME segment, there is no evidence that big data approaches, including additional public or private data, can increase the quality of scoring/risk profiling.

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?

Banks holding any data on SMEs, including clients' credit and financial data, have to keep such data secure and secret. It can only be used for the purposes of lending and for the contractual relationship between banks and their clients. Any sharing of such confidential data requires an explicit mandate by the client and would be done according to freedom of contract.

With PSD2, SMEs can easily provide raw payment data from their payment accounts to non-bank financial service providers, who can develop their own means of analysing data and assessing creditworthiness. Current legislation already enables this, so there is no need for further policy action.

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?

Generally speaking, as cybersecurity is a highly dynamic field, requirements for financial service providers should be principle-based. Any defined single rule would be outdated the moment it is written. Consequently, banks are working very hard to keep track with cybersecurity events. No further regulation is required, and static requirements would have an opposite effect in the dynamic and volatile world of cyber threats.

Cyberattacks are increasingly targeting vulnerabilities in software at the application layer. Software vulnerabilities at this layer are well known (e.g. OWASP Project) but there are no specific

requirements (e.g. security by design) or standards (e.g. A7700 is outdated) for software development and for security mechanisms.

Software or service vendors (especially for financial services) and their subcontractors need to be forced to include security into the whole software life cycle. A way to force them could be to introduce a type of product liability. Certifications and security test results could be used as proof.

There is a lack of standardisation for cross-country Identification and Authentication.

The available security requirements (standards) e.g. ISO 27000 ff, ENISA, BSI group, etc.) cover relevant security topics from an organisational and technical point of view and should be made compulsory.

Standardised software libraries and APIs for critical transactions would be useful to improve security.

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?

Typically, European regulation (e.g. SREP) and national rules (e.g. MaRisk and BAIT in Germany) require reporting of cybersecurity events to public authorities, which in turn can share them with the public. At the international level, the current initiative of SWIFT to enhance IT security and communication between banks is an example of development self-regulatory developments.

Financial service information sharing platforms are already providing specific information to subscribing financial service providers.

There is no legal basis of sharing information among financial services institutions and/or public authorities.

Most paid reports and feeds are customised to the needs of the requestor. Sharing is on the one side not permitted (from a legal point of view), could contain confidential data and on the other side is not necessarily meaningful for the receiver due to different business models.

Cert.at operates an information sharing platform based on MISP (Malware information sharing platform). Organisations and public authorities share information about malware and their indicators. MISP users benefit from collaborative knowledge about existing malware or threats. The aim of this trusted platform is to help improving the counter-measures used against targeted attacks and set up preventive action and detection.

Cert.at in Austria already informs the financial sector in case of nationwide or sector-specific cyber threats.

To improve response to cyber threats at EU level, cross-border information sharing is essential.

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)?

As cybersecurity is a highly dynamic field, requirements for financial service providers should be principle-based. Any defined single rule would be outdated the moment it is written. Consequently, banks are working very hard to keep track with cybersecurity events. No further regulation is required, and static requirements would have an opposite effect in the dynamic and volatile world of cyber threats.

Every provider of financial services should be obliged to perform risk-based cybersecurity testing, which should include:

- Risk assessment with threat modelling of the test objects.
- Regular vulnerability scans of the infrastructure (mandatory).
- Penetration testing, especially for internet facing web applications (mandatory) by an accredited independent provider (whitebox for critical applications).
- Source code audits for critical code parts (mandatory).
- SAST and DAST scanning during development and testing (optional but mandatory for critical applications).
- Incident response training (mandatory).
- Crisis training including business units (mandatory).

ENISA Cyber Europe should be extended. The ratings of the nationwide trainings should be standardised to be comparable between different Member States.

Because penetration testing is mostly scenario-based, there is no easy way to build common standards or frameworks. What tests include and how they are implemented depends mostly on what kind of environment and what kind of scenarios are in scope of testing. Currently most of the companies offering penetration testing perform well and follow international best practices and methodologies (like SANS, NIST or OWASP). In addition, these practices and methodologies could form a common EU ground for the elements addressed.

PCI DSS (Payment Card Industry Data Security Standard) has described pen-testing requirements well. It mandates how often and what is the scope, but gives companies freedom to choose testing providers as well as the methodology that best suits each company's environment. Resilience testing and related requirements are equally important as penetration testing. If a service provider is a Critical Infrastructure Provider in current given country, compliance with such regulations are already required by local authorities.

Generally there is no need for new regulation or new requirements, but we should use current standards and requirements and have common agreement on how we value them and what services should fulfill what requirements. Most importantly, whatever rules or requirements are mandated, these should apply equally to all actors – traditional financial institutes and start-ups – to ensure a level playing field.

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?

Banks have been 'heavy users' of information technology for decades and have always implemented technology for the benefit of their customers. For a given technology, use depends on a cost-benefit assessment, which each bank has to perform in its own individual context.

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
X	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?

All future developments are always uncertain and depend on 'trial and error' in the market.

The example of Bitcoin shows that technology-based innovations can potentially not be captured by regulation even though they practically bypass a highly regulated market. Regulators should ensure a level playing field in all directions. Unnecessary entry barriers should be avoided while existing regulation needs to be enforced.

Regulation should be: (i) principle-based rather than rule-based; (ii) proportionate; (iii) consistent; (iv) balanced; (v) fully technology agnostic; and (vi) required only when justified by measurable data about any kind of misconduct or market misuse.