EUROPEAN COMMISSION
Directorate-General for Financial Stability, Financial Services and Capital Markets Union

Financial services policy and International affairs

Summary of contributions to the 'Public Consultation on FinTech: a more competitive and innovative European financial sector'

This document provides a factual overview of the contributions to the 'Public Consultation on FinTech: a more competitive and innovative European financial sector. The content should not be regarded as reflecting the position of the Commission.

Contents

ANNEX:

1. INTRODUCTION

On 23 March 2017, the European Commission launched a public consultation entitled "FinTech: a more competitive and innovative European financial sector". The consultation closed on 22 June 2017. The purpose of the consultation was to seek input from stakeholders to further develop the Commission's policy approach towards technological innovation in financial services.

The consultation was structured along four broad policy objectives:

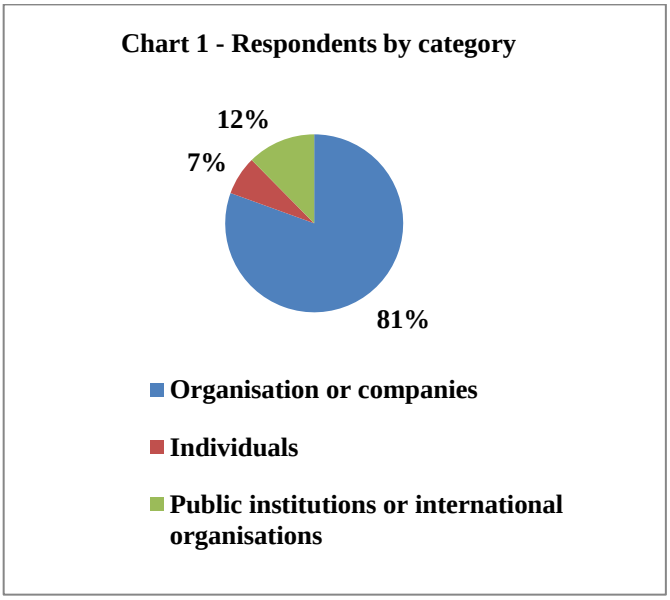
- fostering access to financial services for consumers and businesses
- bringing down operational costs and increasing efficiency for the industry
- making the single market more competitive by lowering barriers to entry
- balancing greater data sharing and transparency with data security and protection needs

The Commission received 226 responses to the consultation and would like to thank respondents for their contributions. This feedback statement provides a factual overview of the contributions received. Any positions expressed in this feedback statement reflect the contributions received. They do not necessarily reflect the position of the European Commission and its services. A summary of the contributions received to the individual questions is set out in Annex.

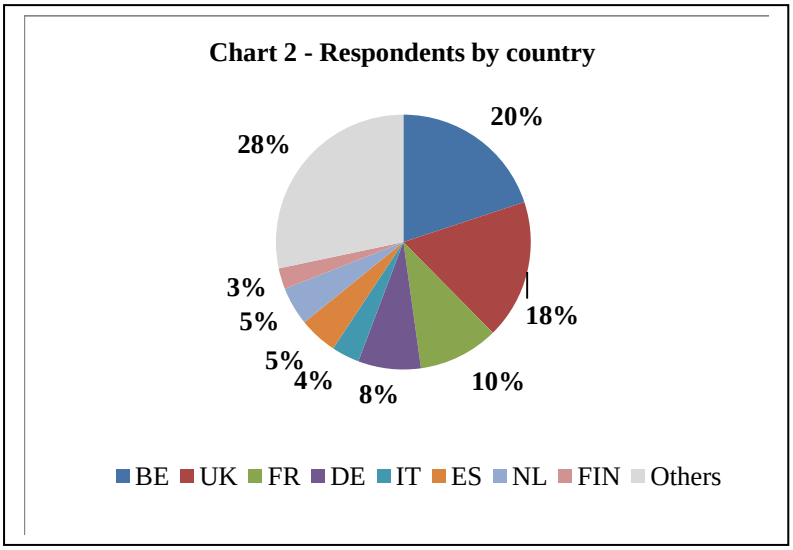
2. KEY MESSAGES EMERGING FROM THE CONSULTATION

2.1. Who responded?

The majority of responses came from the industry (182), mainly from firms and industry organisations. Mainly incumbents and organisations representing them contributed including banks, investment firms, trading venues, insurance, payments and market infrastructures. From the side of start-ups, some FinTech organisations responded as well as a couple of firms. Contributions were also received from technology companies, cloud service providers and consumer or investor organisations and trade unions. 28 public authorities responded to the consultation, including the three European Supervisory Authorities. A limited number of private individuals (16) also contributed.



Respondents were from 22 Member States, with more than half based in four countries, Belgium (45), UK (40), France (23), Germany (18). 16 respondents were based outside the European Union.



2.3. Key messages

Many respondents underlined that FinTech, and technological innovation in general, were drivers of financial sector development. There were huge opportunities in terms of access to finance, operational efficiency, cost-saving and competition.

Distributed ledger technology, big data analytics, artificial intelligence and cloud computing were highlighted as technologies meriting authorities' attention, for which certain initiatives at EU level in the short or mid-term may be considered.

On the risk side, the predominant themes raised were cybersecurity, the use and control of data and money laundering.

Technological neutrality, proportionality and integrity were considered to be the right principles to guide the EU approach to FinTech. Respondents called for applying the "same service, same risk, same rule" principle to all market players, hence ensuring a level playing field in the financial sector.

The need for an open dialogue between regulators, supervisors and firms, whether start-up or incumbent, was stressed throughout the consultation.

The main areas where respondents expressed broad support for EU level action were:

- a clear EU Framework for crowd- and peer-to-peer financing
- more clarity and convergence across the EU on how supervisors handle licencing, outsourcing, in particular to cloud services, and support for innovation (e.g. innovation hubs)
- more developed interoperability and standardisation, and
- enhanced cybersecurity

Other areas where EU action was seen as potentially beneficial to promote the uptake of technologies still at an early stage were:

- assessing the most critical challenges (e.g. technological, regulatory) and possible solutions for the implementation of disruptive technologies (e.g. Distributed Ledger Technologies; artificial intelligence) in financial services.

3. SUMMARY OF RESPONSES

3.1. Fostering access to financial services for consumers and businesses

The vast majority of respondents had a positive assessment of FinTech applications and noted that FinTech solutions were progressively used across a wide range of market segments. The promising use of FinTech solutions for compliance purposes ("RegTech") was also frequently mentioned by firms and public authorities. In addition to enhanced consumer experience, convenience, competition and lower costs, FinTech was seen by a large majority of respondents as providing solutions which contributed to improving access to financial services.

Artificial intelligence and big data analytics for automated advice and execution

Almost all respondents agreed that automated advice was still at an early stage of development and was not equally spread across sectors or across the EU. However, more than half of the respondents considered that it had the potential to reach a greater number of customers, thus enhancing financial inclusion. Some limitations were already identified, such as the absence of comprehensive solutions to tackle complex situations, as well as the need for human intervention in some cases. Respondents' views were divided on the need for common rules for oversight of automated decision- making. Those in favor pointed to risks (e.g. discrimination) and difficulties with respect to supervision. Those against enhanced oversight pointed to the existing frameworks that were considered sufficient (e.g. the current Directive 95/46/EC; General Data Protection Regulation (GDPR), which will become applicable in May 2018, Solvency II and MiFID II) and took the view that it could be premature and might risk stifling innovation.

With reference to the amount of information that should be included in algorithms for investment decision, industry respondents and public authorities called for technologically-neutral approaches. Existing provisions in sectoral legislation (e.g. MiFID II) should apply equally to human and machine-supported decisions. All respondents underlined the applicability of the GDPR's provisions for customer data, including user consent and the right to an explanation for algorithmic decisions. Public authorities and civil society organizations insisted on the data minimization principle, while some industry respondents argued that access to more data could lead to better services.

With regard to new risks stemming from the use of artificial intelligence and big data analytics in financial services, respondents identified mainly risks associated to cybersecurity, data protection, discrimination, lack of transparency and liability issues. Suggested main possible solutions to mitigate those new risks were: a robust cybersecurity strategy, adequate controls in the use of data, a high level of privacy, same requirements as applied to human advisors and a clear liability regime in case of legal disputes linked to advice received via fully automated tools.

Social media and automated matching platforms: funding from the crowd

With respect to the current development of crowdfunding in Europe, most respondents believed that national regulatory regimes hindered cross-border crowdfunding activity and that a EU-level harmonisation was therefore required. Among the potential areas for harmonisation cited were platforms' disclosure requirements, registration requirements and consumer and investor protection rules. Those against further harmonisation argued that the sector was already fully regulated, for example under MiFID, and did not require further European-level action.

A large majority, across all stakeholders, proposed a pan-European framework which should balance the dynamics of the industry and the protection of investors. The framework should be simple and proportionate, should introduce a joint terminology and foster the cross-border market. To support further FinTech solutions in this field, a number of respondents suggested developing regulatory sandboxes with harmonised criteria so that solutions developed in one Member State could be passported.

Almost all respondents agreed that a high level of transparency was instrumental to ensuring credibility and development of new business models. To achieve this, many respondents supported self-regulatory initiatives and rejected additional public regulatory intervention, while others were of the view that this would not be sufficient. Some respondents referred to recent disclosure requirements in EU legislation (e.g. KID, PRIIPs and UCITS style) or national legislation as good examples in this respect.

Sensor data analytics and its impact on the insurance sector

Respondents identified a wide range of applications of sensor data analytics in financial services, in particular in the insurance sector. While respondents highlighted the opportunities to better assess risks, provide more accurate pricing and offer innovative products, respondents also pointed to the risk of exclusion and unaffordable pricing. Examples of price discrimination through the use for example of big data in the insurance sector (e.g. health insurance based on volume of physical activity per day) were raised.

Key issues identified by respondents concerned the reduction of risk pooling, which might fundamentally alter the structure of the insurance industry as well as the weak level of transparency in risk profiling, the risk of privacy unravelling and the aforementioned exclusion risk. The main solution identified by respondents was to ensure that adequate regulation was in place and enforced to protect individuals (e.g. the current Directive 95/46/EC and the upcoming General Data Protection Regulation).

3.2. Bringing down operational costs and increasing efficiency for the industry

The vast majority of respondents viewed favourably the potential of technology to reduce operational costs. The technologies most cited were cloud computing, robotisation and machine learning, Application Programming Interfaces (APIs), Distributed Ledger Technologies (DLT) and remote identification technologies.

While some respondents proposed a wide range of measures that could be taken at EU level to facilitate the uptake of the most promising use cases, others called on the European Commission to be cautious and to avoid premature regulation.

RegTech: bringing down compliance costs

A large majority of respondents believed that RegTech could contribute to reducing compliance costs and making internal risk management systems more efficient. The areas most often mentioned were: anti-money laundering, know-your-customer requirements, fraud and market abuse detection and supervisory reporting.

Industry respondents considered that policymakers should adopt a supportive approach to RegTech as a way of encouraging take-up by industry, improving efficiency and reducing costs. The majority of public authorities welcomed an open dialogue on RegTech with industry and more coordination with other authorities to ensure a consistent attitude towards the use of RegTech-solutions for compliance purposes.

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

A vast majority of respondents expressed concerns about using cloud services due to a lack of clarity regarding their use in financial services, a lack of harmonisation between national rules and different interpretations of European rules by national supervisors.

Various interpretations of personal data handling across the EU and data localisation restrictions were obstacles identified in most contributions.

A significant number of respondents pointed to the need for Cloud Service Providers to adapt their offer to specific constraints of financial institutions (e.g. audit obligations).

The high concentration of Cloud Service Providers was considered as a source of risk by some respondents.

To tackle these issues and support the adoption of cloud computing by financial services providers, some respondents were in favour of a limited intervention at EU level (e.g. high-level principles at EU level but guidance from national supervisors), while others called for stronger intervention to ensure legal certainty and harmonise rules in using cloud services (e.g. EU requirements for cloud services that could become standards for international cloud computing agreements).

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

The overwhelming majority of respondents were convinced that DLT offered opportunities in many different areas, such as: securities; payments; insurance; anti-money laundering and know-your-customer requirements; record-keeping; reporting; crowdfunding; Initial Coin Offerings (ICOs); digital identities; central bank money, post-trading, and financial data sharing. In some cases, respondents provided concrete examples under development (e.g. European consortium of financial institutions exploring the development of a post-trade blockchain infrastructure for SMEs).

According to a vast majority of respondents, the main challenges for the implementation of DLT solutions are data standardisation, interoperability of DLT and scalability.

With regards to the main regulatory challenges raised by DLT, public authorities identified various issues, among which the question of the validity and enforceability of smart contracts[1], together with the classification of tokens exchanged on DLT were mentioned. In the future, while DLT-based solutions move from proofs-of-concept or pilot to full market implementation, some authorities also indicated that EU financial services legislation may have to be adapted.

A large majority of companies provided similar views as public authorities and cited securities law, GDPR, enforceability of smart contracts, the nature and financial classification of tokens, liability rules, standardisation, validity of blockchain elements, regulators' understanding of the technology, but also governance of DLT networks as main issues that required attention or clarification. Besides, a number of industry respondents acknowledged that DLT was still at an early stage of development and some stakeholders noted that any regulatory measure on DLT would be premature in the short-

[1] A smart contract is a piece of code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced.

term. Some stakeholders also referred to regulatory sandboxes as a useful tool to overcome the identified issues and help regulators keep up with change.

Outsourcing and other solutions with the potential to boost efficiency

The majority of private sector organisations considered that the current outsourcing rules constituted an obstacle to reaping the full benefits of outsourcing functions to FinTech, referring most often to outsourcing to cloud services.

On the other hand, the majority of public authorities considered that the current outsourcing frameworks were adequate and did not require major changes. Several authorities however recommended updating specific guidelines or providing more guidance in view of FinTech developments.

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

The vast majority of respondents agreed that technological neutrality, proportionality and integrity were the right principles to guide the EU policy and regulatory approach to FinTech activities.

Most respondents insisted on the "same activity, same rule" principle to ensure a level playing field between all market participants. They also found that open discussions and collaboration between the industry and regulators/supervisors were essential to support FinTech uptake in the EU.

The majority of respondents were in favour of more proportionality in the regulatory framework for financial services and suggested criteria in this respect (e.g. business model, size, systemic significance). However, very few specific examples of insufficient proportionality were provided.

Role of regulation: licensing, proportionality and outsourcing

Regarding more specific regulatory barriers that might prevent FinTech firms from scaling up across Europe, respondents mostly mentioned:

- the lack of harmonised anti-money laundering rules and their various interpretations across the EU (e.g. Know Your Customer requirements in a digital environment)
- non-technologically neutral provisions in financial services legislation (e.g. paper disclosure requirements; prudential treatment for software in CRR/CRD)
- the restrictions on data movement stemming from various national legal or administrative requirements, hindering the uptake of new technologies.
- the complex combination of national and European legislation for crowdfunding and peer-to peer platforms limiting cross-border activities

Public authorities had mixed views on the need to introduce new licensing regimes for FinTech activities. Some considered the current regimes to be sufficient, while others claimed that crowdfunding and peer-to-peer activities in particular needed a more harmonised EU framework.

On the industry side, banks and payment services providers generally considered that current activities are well covered by existing licensing regimes. Most gaps seemed to be concentrated in investment services and non-bank lending, where a number of firms and consumer organisations called for a clear EU framework for crowdfunding. Other areas mentioned by stakeholders related to e.g. licenses for digital asset managers, aggregators,

brokers, invoice and supply chain finance or advice and intermediation in the insurance sector.

Most respondents welcomed the upcoming GDPR that will address some of the data-related issues but underlined that those new rules would need to be further clarified. They insisted on the need to properly implement an EU free flow of data initiative in the financial sector.

Role of supervisors: enabling innovation

The vast majority of respondents called for a stronger role for the ESAs vis-à-vis technological innovation. They suggested that the ESAs could coordinate innovation hubs and regulatory sandboxes which had been recently set up by national supervisors, share best practices and enhance supervisory convergence. Most respondents claimed that the ESAs should build up competence in a number of areas such as cloud computing, big data and cybersecurity. ESAs should also enhance cross-sectoral work, since FinTechs often operate beyond traditional sectors.

While the majority of respondents favoured more harmonised approaches for regulatory sandboxes at EU level, industry respondents and public authorities had diverging views. Most industry respondents called for a common European framework harmonising national approaches, be it through high-level guidelines or through a dedicated EU legal framework. On the other hand, most public authorities were not in favour of an EU sandbox and favoured national initiatives or stronger coordination by the ESAs. Some authorities expressed opposition to the idea, considering it incompatible with a stability and consumer protection mandate.

Finally, almost all respondents supported the idea of setting up an Innovation Lab, established by the European Commission, to share practices and discuss the possible regulatory and supervisory concerns stemming from the uptake of new technologies.

Role of industry: standards and interoperability

Most respondents underlined that interoperability is a priority for the FinTech market, and that further standardisation is needed. Standards and technical specifications should be developed by market participants and by the industry, and the use of global standards should be promoted, as opposed to national or regional standards. A majority of respondents promoted the adoption of an open source model where libraries of open source solutions would be made available to developers and innovators.

Securing financial stability

Regarding the expected impact of Fintech on the safety and soundness of incumbents, almost half of all respondents thought that this impact depended on the extent to which FinTech complemented or competed with established market players. Almost half of the companies foresaw a huge impact of FinTech solutions which may affect the entire financial services value chain and considered FinTech as a key driver to improve the efficiency in almost every area of financial services. FinTech solutions played a key role in reducing inefficiencies, boosting higher levels of automation, leading to more efficient back office activities, higher levels of transparency, operational resilience and significant cost-reduction.

3.4. Balancing greater data sharing and transparency with data security and protection needs

Storing and sharing financial information through a reliable tool

Almost all respondents underlined the potential of DLT to store and share financial information. It could provide benefits such as decentralisation, flexibility, transparency and immutability.

Regarding digital identity frameworks specifically, a majority of respondents stated that there was no mature digital identity framework at the moment to be used with DLT or other technical solutions in financial services. Some respondents however recommended that digital identity frameworks could be further promoted, since they were the most important enabler for FinTech. In this respect, most respondents referred to the need to implement the e-IDAS regulation, the revised AMLD and the GDPR and to ensure that the private sector can access the e-IDAS framework. Others suggested introducing a common digital identity in the EU.

Finally, the vast majority of respondents also highlighted significant challenges to use DLT with regard to relevant legislation on the protection of personal data. Right to be forgotten, confidentiality and cybersecurity were the challenges most often mentioned by respondents. A number of possible solutions were suggested either to limit the access to data by users in a DLT-based infrastructure or to limit data availability in the blockchain.

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

Respondents provided a number of examples where big data analytics combined with technology-based solutions create opportunities for the risk-profiling of SMEs (e.g. the access to SMEs bank account data, data aggregation, scoring engines). With regard to sharing credit and financial data with alternative providers, most respondents agreed that the implementation of PSD2 and GDPR will be instrumental. As a result, respondents from the banking industry considered that no additional action was necessary in this area. Other respondents suggested other initiatives, such as setting up public data repositories in full compliance with data protection rules, adopting common standards to get a clearer framework or promoting the exchange of best practices. The main risks identified by respondents included cybersecurity and lack of confidentiality for SMEs.

Security

Many respondents argued that all financial markets players, taking account of the activity performed, should be subject to the same cybersecurity requirements. Moreover, respondents called on the Commission to provide guidance on the possible means to enhance information sharing among market participants, in particular as regards compatibility with the GDPR. With regard to cybersecurity stress testing, there was broad support to ensure more regulatory and supervisory convergence at European level, as well as the mutual recognition of tests across jurisdictions and between supervisors.

ANNEX: Summary of feedback received per question