EMF-ECBC Position Paper
European Commission's Public Consultation on FinTech: A More Comprehensive and Innovative European Financial Sector

15 June 2017

1. Introduction

The European Mortgage Federation-European Covered Bond Council (EMF-ECBC)[1] welcomes the opportunity to comment on ''Public Consultation on Fintech: A More Comprehensive Innovative European Financial Sector'' which was launched by the European Commission on 23 March 2017.

2. Specific Comments

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?

Based on the feedback received, it appears that some banks have recently begun to cooperate with FinTech companies with the objective of obtaining enhancing specific key business areas, products and/or services by leveraging on the following:

- Solutions focusing on cost-reduction via improvement of processes or replacement of platforms/IT solutions by leveraging on edge-cutting technologies; and
- Solutions enabling banks to attract new customers, to improve customer relationships or to increase the offering of new and innovative products/services. Therefore, the availability of more FinTech solutions are welcome in areas such as corporate and investment banking, core IT banking solution, and solutions focused on enhancing the data quality and data architecture.

More precisdely, the following FinTech applications are considered most popular among banks: Neo Bank (digital money), API, Lending, Payments, Cyber Security (Fraud Detection and Data Protection) AI applied to Process Automation(RPA), AI applied to Robo (advisory/ for advisory), AI applied to Regulatory (Regtech).

Overall, it could be said that start-ups and small non-banking FinTech companies offer the larger players within the FinTech cluster a new way of conducting product development and innovation. This new approach to product development and innovation is now also being adopted by large incumbent banks at a growing pace and magnitude.

Finally, we would like to take this opportunity to underline the impotrance of a level playing field – same business, same risks, same rules – to ensure consumer protection and financial stability, irrespective of who the service provider is.

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.)? 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.

[1] Established in 1967, the EMF is the voice of the European mortgage industry, representing the interests of mortgage lenders and Covered bond issuers at European level. The EMF provides data and information on European mortgage markets, which were worth over 7.0 trillion EUR at the end of 2015. As of October 2016, the EMF has 19 members across 14 EU Member States as well as a number of observer members. In 2004 the EMF founded the ECBC, a platform bringing together Covered bond issuers, analysts, investment bankers, rating agencies and a wide range of interested stakeholders. As of October 2016, the ECBC has over 100 members across 26 active Covered bond jurisdictions and many different market segments. ECBC members represent over 95% of Covered bonds outstanding, which were worth nearly 2.5 trillion EUR at the end of 2015. The EMF-ECBC is registered in the EU Transparency Register under the ID Number 24967486965-09.

Automated financial advice is in the process of developing, albeit at a relatively slow pace. The benefits of automation in the financial industry sector are clear. On the one hand, FinTech companies contribute to the lowering of the price of financial advice and on the other, there is a wide range of choice in terms of services offered and better tailor-made options for consumers which increases the customer base. However, as this kind of solutions is still relatively new, it is too early to determine whether automated financial advice solutions will increase the customer base in reality. Despite the fact that automated financial advice is still in the first stages of its development, some financial institutions have already started collaborating with start-ups offering this kind of service.

There is also a human factor here. Not all consumers find traditional face-to-face advisory meetings useful or convenient or value a personal relationship, but rather prefer a digital approach. In view of this, while for some consumers a solely digital interaction is a way to enhance financial inclusion, for others face-to-face interaction could be considered vital.

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? 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.

Overall, it is in the interest of financial institutions that the algorithms used are reliable and scientifically proven and that the results are interpreted correctly. Due to this, the staff of financial institutions should ideally have the required expertise on the topic. Furthermore, due to the high level of regulation of the financial services sector, it might be necessary for the relevant regulatory and supervisory authorities at national level to acquire the same competences in order to understand and validate the algorithms. Therefore, a system of control and transparency of artificial intelligence (AI) algorithms could be established. At the same time, the particular way in which this technology works should be taken into account.

One particular advantage provided by AI is to find better and different paths when data is analysed, in order to predict accurate actions and consequences. The way in which AI systems do so is the result of a series of complex computational operations that could make it almost impossible to check some of the middle stages in the decision-making process of the machine-performing AI.

In view of this, an effective way to guarantee transparency and control should be pursued, without sacrificing the notable and remarkable potentialities of this technology.

One way to guarantee transparency and control in AI is to check and monitor the data sources and the final results of a certain operation made by AI. The following elements should be checked: (a) the data processed by the AI and (b) the produced result, verifying how the system works by way of customised tests. Transparency and privacy issues around the algorithm are of key importance to the customer and they should be verified by specific approval tests, back testing, involvement of the compliance and risk management services, market abuse controls, etc.

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)?

From the point of view of the service users, it is important that the service providers are clear about which kind of information is being considered in the algorithm. The minimum amount of information to be included can vary according to the functionalities of the service and the purposes of the solutions but should be in line with current regulations e.g. GDPR. The basic information required about the client and his portfolio, in terms of knowledge and experience, financial status, investment timeframes, risk acceptance and investment goals, for example, is usually included within the risk profile. Such information is considered necessary for the performance of the automatic reset function by the personal banker, which allows the matching of the client real portfolio with the recommended portfolio.

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?

Overall we believe that 'big data' and AI will provide benefits to the Consumer. However, from the consumer's perspective, risks could be linked to unfair policies or incorrect profiling resulting from erroneous/incomplete data analysis, interpretation or application of algorithms, incomplete or incorrect information on the use and functioning of the instruments, for example. It is therefore advisable that consumers should be first properly informed and their consent obtained in order to start the processing their requests via artificial intelligence. However, there is always the risk that atypical cases are excluded.

To avoid these risks, a policy of transparency towards the customer concerning the algorithms used could applied. Also, an external validation of the algorithms, especially in heavily regulated environments, could be helpful to address these risks. Besides cybersecurity and data protection, which are common challenges to all IT services offered nowadays, the biggest challenge that artificial intelligence could face in the future is related to the definition of legal liability for each actor involved in a given service (e.g. cognitive engine provider, system integrator, company offering the service, user of the service, etc.). In principle, each actor should be held liable for his own actions and decisions made, as well as for the results or outcomes produced from the service. However, the most difficult part is the identification of which actions caused certain outcomes.

In addition, in order to address the above-mentioned challenges, some of the measures to be taken into account could be the requirement of a certification of cognitive engines, the monitoring of training activities and the monitoring use of the applications, for example.

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

There are many different legal frameworks across the EU relating to crowdfunding, which could be to the detriment of consumers and investors. Common rules for crowd-funding and other similar financing channels at EU level could therefore be beneficial.

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?

Regarding non-banking financing and related activities, the Commission should ensure the principle of a level-playing field in terms of regulation and supervision in order to guarantee consumer protection and maintain financial stability.

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?

With the view of ensuring consumer protection, the level of transparency imposed on fund-raisers and related platforms should be the same as the one required for banks and insurance companies. Therefore, consideration should be given to a common regulatory authority for all banking, finance and online payment services.

In addition, platforms for lending crowdfunding and invoice trading should periodically publish the registered default rates. The rating of the crowdfunding platforms could be subsequently established via European legislation.

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?

An example could be given with biometric technologies to sign contracts, to simplify UX, authentication and identification. In our view, the use and application of Distributed Ledger Technology and "Smart Contracts" can potentially enhance specific businesses of the Bank (e.g. trade finance) and general areas (e.g., IT Core banking).

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?

Based on the feedback received, some of the most promising use cases of FinTechs to reduce costs and improve processes are as follows:

- Trading platforms that reduce costs while increasing markets transparency;
- Platforms used in capital markets to access data in a simpler and more efficient way;
- Digitalisation of processes that facilitate the interaction with customers;
- Cloud computing;
- Robotics to reduce costs by re-framing existing processes to E2E processes;
- Distributed ledger technology/blockchain could be a technology which assists the processes between parties who need to improve the information exchanged, particularly where no dedicated infrastructures exist;
- Big data;
- Artificial intelligence,
- Voice Technologies, and
- Biometrics.

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?

It is possible that the recruitment of employees with specific competences on science, technology, engineering and mathematics will increase. Employees with skills to develop/maintain legal and ethical aspects of artificial intelligence will also be needed. EU Data Protection law and Banking regulation could evolve vs. a more assertive/directive approach towards national regulators in order to better support seamless and paperless processes (digitalisation).

The EU should be able to be flexible enough, as well as adaptive, in the face of a very dynamic market environment, which could be challenging. Therefore, once again, it is important to maintain a level playing field regarding regulation across potential competitors/sectors in the EU Members States in order to ensure consumer protection and financial stability.

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?

Collaborating with FinTechs involves an open-minded approach, a certain degree of adaptability, fast execution and a long-term vision. In view of these considerations, automation and innovation do not necessarily mean a reduction of employment.

However, digitalisation may provide an added-value by reducing costs regarding the storage of data which would be less expensive than storing and maintaining paper archives in specifically designated premises, for example. Digitalisation can also reduce the cost of personnel that perform repetitive activities which would lead to performance of higher quality. In view of this, there could be a shift in staff positions impacting primarily back-office employees and becoming more significant in the long-term.

Having these considerations in mind, firms in the financial industry could face the challenge of not being able to ensure that current employees are able to adapt to a more digitalised working environment. Therefore, the availability of appropriate training for employees is important.

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?

Among the most promising use cases of technologies for compliance purposes are the following:

- KYC/UBO platforms leveraging on breakthrough technologies;
- Cognitive technologies applied to: mapping of regulations/policies and its consequent impact assessment, transaction monitoring, market abuse and trade activities;
- Automation of compliance reporting;
- AML/CFT;
- Automation of control activity related to non-compliance risk, through data analytics as well, and
- Automation of the risk assessment analysis, by using AI tools

The main obstacle to the development of such solutions, however, is the low level of data and process standardisation. Therefore, the adoption of common standards in the deployment of the regulation can help the development of RegTech solutions. However, although compliance practices could be facilitated by technology, too much standardisation of procedures, especially with respect to credit authorisation, for example, is not desirable.

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

Overall, the security of cloud computing services could be improved. The majority of cloud computing services providers are based in the US and therefore the applicable data protection laws appear to be less protective of confidentiality compared to the related national laws at EU level.

Question 2.6.1: Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with? Please elaborate on your reply to whether commercially available cloud solutions do meet the minimum requirements that financial service providers need to comply with.

The available cloud solutions do not require binding contract clauses for financial services; the contract clauses are standard for all their customers. Even the use of OTC instruments appears to be risky due to significant differences that could occur as a result of wide market movements (i.e. swap as opposed to futures and bonds). The use of DLT is possible in the post trade but the importance of the different DLT should be highlighted, otherwise the risk is the creation of some separations that will affect the development of the markets and limit liquidity.

The establishment of common certification rules could be beneficial at EU level, in order to reduce the large amount of work that is being done in every mortgage bank in order to ensure that a given cloud solution is compliant with the supervisory requirements.

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

The security and confidentiality of the data stored in the cloud is essential and should be unequivocally guaranteed for both consumers and businesses.

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

The DLT can provide a single source of information where SMEs can share their financial data (obviously complying with existing regulation, starting from GDPR) in order to help financial institutions to better assess their credit risk. This could make it easier for SMEs to access banking services and especially financing services. In the short term DLT is used mainly with crypto currencies, which could improve the international trade for SMEs. Other DLT applications are at POC stage. In the long term, the trade finance DLT platforms will benefit the international trade of goods providing advantages in terms of time reduction, costs and trust of the system.

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)?

Based on the feedback received, it appears that a holistic approach could be beneficial. Furthermore, to exploit the full potential of the technology and to guarantee legal effects for cross-border transactions, a strict coordination among different jurisdictions should be foreseen.

With regards to data standards and governance, DLT and smart contracts need to be underpinned by some level of data standardisation and governance in relation to the formation and maintenance of such standards. This will help reduce complexity and support scalability, particularly given the need for interoperability with existing infrastructures and also to provide a common underpinning for the multitude of DLT solutions and smart contracts.

In addition, even limiting the focus to the financial industry only, beyond blockchain/DLT, other issues should be also considered, such as privacy, big data, cyber security and internet of things, amongst others. The great challenge for the usage of DLT concerns the creation of shared tech operational standards that are compliant with the various national regulations. The issues must be managed by institutions able to set standards, timeframes and rules. Otherwise, there is the risk that different priorities for the individual countries limits the effectiveness and the establishment of shared standards and regulations (digital identity, sandbox and cyber security, for example).

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?

At this stage, a cautious approach to DLT technologies is advisable, due to the fact that the impact these technologies could have on the services provided by banks as well as what the potential regulatory obstacles could be, if any, remain unknown.

Nonetheless, if European and international regulators decide to update the regulatory framework considering the DLT, in order to allow the financial industry to exploit the full potential of DLT, a homogenous legal framework at national, EU and international levels is needed. This being said, we tend to agree with ESMA's view that currently there are no major impediments in the EU regulatory framework that would prevent the emergence of DLT in the short-term. In this respect, we support ESMA's view that any regulatory measure on DLT would be premature in the short-term.

However, it appears that the level of consumer protection sought by legislators and regulatory authorities is the main obstacle for the development of modern financing. The ever-increasing demand for consumer protection could lead to an increase in the required information, procedures, reporting and storage standards in the financial sector, which does not necessarily guarantee the required levels of security.

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

Italian banking regulation, for example, requires the bank to maintain internal skills to potentially reintroduce the key outsourced functions (FOI). Moreover, the regulation does not provide any specific provision for trial runs and solution testing. This and several other requirements are a serious obstacle to increasing current outsourcing, despite FinTech. In

France, the legal framework is cumbersome, but this environment is managed by outsourcing establishments - so normally it should not be a hindrance. Harmonised EU level guidance could be of benefit in developing a more effective framework.

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

Based on the feedback received, the existing outsourcing requirements in the financial services legislation seem to be sufficient, however the added value of potential future requirements that contribute to further technical progress could be assessed.

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?

Blockchain has the potential to increase efficiency for financial service providers and potentially also for a number of other industries. Currently the use cases which are tested the most relate to capital markets, trade services, digital identity/KYC and cross-border payments.

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?

One best practice example is the UK FCA's innovation hub and the application of a regulatory sandbox in finance (more information available here). Another is IDA Ireland, which is an agency responsible for the attraction and development of foreign direct investment (more information available here). In relation to regulation relating to the establishment of a financial institution (for the purposes of the calculation of capital requirements for the establishment of a financial institution - see for example the case of the soft/full e-money license in UK) and regulation regarding data privacy protection, a harmonised user experience is required to guarantee a level playing field.

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

The most efficient path for FinTech innovation and uptake in the EU is to conform to the best practices used in each Member State in order to make the EU more competitive and to provide incentives for the development of the markets in individual EU countries. RegulatorS should create the conditions for this, i.e. ad-hoc financial products, incentives, etc.

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?

Different market actors, whether banks or start-up companies, should ideally be subject to the same regulatory rules. This holds true as a result of the fact that start-up companies could pose risks to consumers, despite the fact that they are limited in number and size. One of the risks that start-ups pose relates to mismanagement. The respective regulators and/or supervisors should be more active in helping and supporting start-up companies in their management, without, at the same time, placing banks at a disadvantage.

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

The issuing of more coherent licenses and a more uniform deployment among the various Member States is needed. Possible consequences relate to the alteration of market dynamics in favor of countries that require very different and more favorable features (i.e. assets, for example).

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

It would be beneficial if the European Supervisory Authorities (ESAs) were to establish regulatory standards for a common level playing field at EU level.

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?

It would be desirable to have more favorable regulations with respect to the establishment of innovative start-up companies and FinTech firms. These regulations, however, should ideally ensure that Member States can issue licenses with features that are fit for the activities that are performed. At the same time, the regulatory framework at hand should not create unfair competition vis-a-vis banks that also use similar technology in the provision of financial services.

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?

Certain issues should be considered when implementing the free flow of data in the Digital Single Market, such as:

- Cloud Services;
- The currency specified in the contract (euros or another currency) and the related foreign exchange risk;
- The law applicable to the contract at hand (which could be different from the law applicable in the country of the consumer);
- The language of the contract.

Additional issues could relate to the costs associated with blockchain and the involvement of third parties.

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

While the main aim of these three principles is to protect the consumers and to combat money laundering and terrorism financing, more uniformity in the application of the rules and regulations related to FinTech could be beneficial.

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?

Regulators should interact with organisations, such as The Global FinTech Hubs Federation (more information available here), for example, in order to cooperate and exchange information on best practices used at the international level.

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?

The idea of an Innovation Academy needs further analysis. We believe that positive incentives to promote digital business models could be set by Institutions.

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

The idea of a regulatory sandbox needs further analysis.

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

The idea of a regulatory sandbox needs further analysis.

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

Possible measures could be the provision of needed financing or tax-cutting for hubs and innovative firms, i.e. start-up companies or established firms that invest in FinTech projects either directly or through in-house development, or through the acquisition of know-how from the market, by founding start-ups or by buying patents and stock options.

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?

The level of data and process standardisation appears to be one of the main obstacles for the development of RegTech and FinTech solutions. The definition of shared standards, which could be challenging to use with highly innovative services and processes, could be more easily applied to already exiting situations. EU-wide authentication, however, could have an impact on onboarding practices and procedures.

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?

Standards at EU and global levels could facilitate the efficiency and interoperability of FinTech solutions by reinforcing automation in the exchange of data flows between FinTechs and regulators, for example. These standards should only be defined, and not strictly imposed, in order to provide added-value to the processes and to decrease the costs of the system, while leaving it to the market to determine their real effectiveness.

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?

The promotion of open source models could help to create innovative solutions with lower costs. However, innovation as such should not be bound to the use of specific technical solutions in order to deliver its most significant advantages. Ideally, the role of the EU institutions in this field should be evaluated, since, on the one hand, EU regulation may have a role in outlining a standard definition, however, on the other hand, the rapidly evolving nature of technology developments could be an obstacle in this sense.

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.

FinTechs could have an impact on the safety and soundness of incumbent firms, which could be disintermediated in the services that incumbents offer to final customers. However, FinTechs also represent an opportunity for incumbent firms to

develop new partnerships which can create efficiencies in terms of cost reduction, better capital allocation and customer acquisition.

In addition, the development of FinTechs should not be at the expense of normal banking activity. This could result in leaving traditional operators that invest in FinTech activities with a low added-value, which could be to the detriment of consumers.

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 order to develop the Digital Single Market for financial services, the free flow of data should be substantial because it:

- Offers the possibility to deliver tailored products and services, consistent with the actual consumer needs and the customer lifecycle, and
- Complies with the required regulatory rules and risk evaluation.

Moreover, the use of data to analyse the client's profile and predict his behavior in the future is key. Another important goal is to address all personal needs of the client. When processing users' personal data for commercial purposes, banks comply with the relevant principles as outlined in the European data processing laws.

If the objective of the Digital Single Market strategy is to support the development of digital infrastructures and to improve the access to digital services for all, the lawful processing of the users' personal data should be ensured and taken into account.

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 technologies currently used in the financial services industry are already providing reliable tools for storing and sharing financial information. However, such solutions require a central counterparty playing a supervisory and/or administrative and/or notary role. In specific use cases, DLT solutions provide an opportunity to create decentralised networks, where a central counterparty is no longer needed. In such different operating models, participants can share information in a reliable and secure way. In relation to security issues, the management of financial information on DLT systems appears to be less critical because users of the system can be selected and restricted, if necessary. Privacy, however, is of greater importance, because the permissions for reading, writing and authorising the sharing of information are obtained separately.

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

Based on the financial data obtained, the critical factor in the managing of digital identity data on DLT lies in the privacy issues and in the compliance practices with the respective regulation at national level.

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

The challenge lies in finding solutions with shared operating standards between the systems as such, and their international effectiveness.

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?

The sharing of information should be aimed at improving the services that are provided irrespective of whether the clients are SMEs or bigger firms. In order to achieve that, the process of data sharing should be improved, respecting the actual legislation on personal data protection, by adopting common standards, for example.

Question 4.6: How can counterparties that hold credit and financial data on SMEs and other user 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?

The sharing of information can be facilitated through the adoption of shared standards which enable a faster and more effective relevant data flow between firms, i.e. for risk assessment purposes, for example.

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?

A targeted framework could be established to define the terminology in the field, in particular for the handling of IT security accidents, for instance.

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

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

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

A minimum requirement could be introduced around the methodology of the performance of security tests and the handling of the IT security accidents (i.e. by adopting the OWSAP or OSSTMM standard).