UK Finance response – "FinTech: A more competitive and innovative European financial sector"

15 June 2017

Introduction:

UK Finance welcomes the opportunity to respond to the European Commission's Consultation "FinTech: A more competitive and innovative European financial sector" published on 23 March 2017.

UK Finance is a trade association representing 300 of the leading firms providing finance, banking and payments-related services in or from the UK. UK Finance has been created by combining the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association.

Our members are large and small, national and regional, domestic and international, corporate and mutual, retail and wholesale, physical and virtual, banks and non-banks. The interests of our members' customers are at the heart of our work.

Key messages:

Coordination of the EU FinTech Agenda

The attention being shown to the FinTech agenda across the EU is welcome and helpful. The banking industry appreciates the willingness of policy makers and regulators to explore new solutions to existing problems and consider how technology can change the nature of finance for the benefit of consumers and markets.

However, there is currently an extensive amount of work progressing at pace across the EU. Although this will no doubt lead to progress, as with any priority activity, there is a risk of duplication and error if there is not proper coordination. In particular, we would welcome the coordination of consultation activities in order that the industry can dedicate its time to answering questions on specific topics in greater detail rather than duplicating responses across EU bodies.

This interest is also present in other jurisdictions and at the international level. International harmonisation has long been called for, but never has it been as important as it is now in the very moment when innovation in the sector is reaching a new level of intensity and growth. FinTech activities, whoever is engaging in them, have the ability to operate across jurisdictions and many of the companies investing in such technology are also not limited by geographic boundaries or subject to a single legal and regulatory regime. New regulatory and supervisory frameworks should strive to be harmonious with existing innovation frameworks in order to mitigate against conflicting rule sets that may hinder innovation and ultimately create instability in the market and risk for consumers.

Recommendation: The European Commissions' FinTech Taskforce should take up a coordinating role in Europe in order to ensure efficient progress is made on the FinTech front. In addition the Commission should work to coordinate the EU's FinTech agenda with that of the international community including international bodies such as the G20 and FSB as well as other national jurisdictions.

As examples of the activity currently or recently underway in Europe and as sources for further information on Big Data, DLT and Cloud Computing please note the below:

- BBA response to ESMA DLT in Securities Markets discussion paper (Sept 2016)
- BBA response to ESA Big Data discussion paper (Feb 2017)
- Forthcominging UK Finance response to FCA DLT discussion paper (July 2017)
- Forthcominging UK Finance response to EBA consultation on draft recommendations to outsourcing to the Cloud (August 2017)

Strengthening the FinTech ecosystem

Banks have been the main channel of technological innovation in financial services for several decades. Over the course of that time numerous developments, which today would be called FinTech, have been rolled out to consumers and other users of banking services. Examples of this range from the use of contactless payment cards to the various features developed for online and mobile banking including the ability to make mobile payments. Some of these developments would have been obvious to consumers, but others like the development of private cloud computing networks or the use of data to offer more tailored products, which have been underway for some time, remain less visible, all the while benefitting consumers and strengthening markets.

However, these technologies are not always developed exclusively by incumbent firms. Thus, while there are good reasons for banks to rely on internal IT departments, there is also considerable potential to create value — both for themselves and the economy at large — by nurturing an ecosystem of startups and technology innovators that can assist banks in developing shared platforms that increase the resilience and cost effectiveness of banking and payment systems. For example: payment solutions that combine digital payment with real life payment (e.g. smart phone as debit card), or banks using robo-advisory tools to optimise asset management portfolios.

A high percentage of banks view the possibility of partnerships with FinTech companies large and small with great interest. The objective of these partnerships is primarily to obtain concrete benefits that enhance specific key business areas, products and/or services by leveraging:

a) solutions focused on either cost reduction via improvement to processes or replacement of platforms / IT solutions with either new business models or technologies;

b) solutions enabling banks to attract new customers, to improve customer relationships or to increase the offer of new and innovative products/services.

Banks, in turn, have a lot to offer FinTech startups:

- specific financial and markets expertise (risk assessment, evaluation and management)
- scalability owing to their large customer base
- experience operating across regulatory regimes
- the ability to address financing needs.

The strengths of both banks and FinTech startups mean that both will often do better by cooperating rather than by competing.

Banks are thus seeking to collaborate with technology companies, including start-ups, wherever beneficial. Bringing outside innovation into the bank can be an ideal way to enable the deployment of better technologies which ultimately make the market more competitive and improve outcomes for consumers.

Collaboration between banks and startups does not mean that startups are limited in their ability to scale. Companies such as Stripe in the US, which was valued at £9.2bn at the end of 2016, show that technology providers can be major players in their own right even if enabled through collaboration with banks. Ultimately this success is based on the access to customers that banks are able to provide to small technology companies who might otherwise not have the time or resources necessary to grow their market share. In short, startups or scaleups benefit from banks' scale and customers while banks are able to make great use of their expertise in programming and analysing data.

> **Recommendation:** The Commission should continue to support the development of FinTech and the growth of a strong FinTech ecosystem across Europe. As the Commission develops its policy approach to FinTech, the following should be kept in mind:

- A one-size-fits-all regulatory approach is not conducive to technological innovation. Any regulatory framework should be flexible, graduated and principles-based, with oversight tied to scale and the risks presented.

- Associated with this is the need to focus on frameworks and not specific technologies or companies. We will say more on this regarding the specific questions below.

- New rules or guidance should take into account banks' existing authorities to develop, test and launch innovative products and services. It is also important that regulators do not implicitly limit the ability to experiment – there can be no reward without some risk and thus it must be acceptable for some new initiatives not to work out.

- Specific activities warrant careful attention by regulators, regardless of who is engaging in the activity – namely payments, lending activities, and data storage. The risks associated with these activities have far reaching impacts to consumers and the broader financial system (i.e. money laundering, terrorist financing, disparate impact, fraud, identity theft, unauthorized transfers, etc.).

- Regulators and supervisors must be prepared to develop new expertise and engage both banks and non-banks in order to understand the fast moving changes happening in the market. The industry stands ready to assist regulators in knowledge sharing and we look forward to developing a mode of interaction that ensures innovation comes to the market quickly, efficiently and above all, safely.

<u>Big Data is not a new phenomenon</u>

We support the Commission in exploring issues around Big Data and would encourage further understanding the potential benefits of the greater use of data in financial services, beyond the paper's focus on financial advice. In general, improvements in data collection and analytics that we have come to know as Big Data are a natural evolution of the data-driven processes that the financial industry has long used to improve its understanding of consumers/customers in order to better serve them.

Banks and other financial institutions have long been custodians and users of data and have well-established systems and protocols for using and protecting sensitive data on a large scale in compliance with the applicable legal and regulatory requirements. We believe that the risks arising from the use of Big Data are both foreseeable and manageable. Those risks should not diminish the ability of financial

institutions to continue to use Big Data to benefit consumers and customers through, for example, offering automated advice thereby increasing financial inclusion, enhancing cyber security protection, and financial crime prevention through threat detection analytics. We encourage the Commission to focus on providing the right conditions to enable financial institutions to continue to serve their customers in the best possible way by developing Big Data technologies.

Cloud computing and the difficulties of outsourcing regulation:

Cloud computing is increasingly the tool that provides the raw power necessary to use innovative technologies and business models that have the potential to disrupt the traditional banking model, providing value to consumers, increasing business efficiency and potentially enhancing market security. The most notable technologies that will benefit from cloud computing are data analytics, machine learning and distributed ledgers. In addition, many of the technology startups providing technology solutions to the banking industry or directly to consumers take a "cloud first" approach meaning that enabling greater and more efficient use of cloud computing will have direct benefits on innovation and competition in financial services.

As the market is developing, it is increasingly possible to view Cloud as more akin to a utility than third party outsourcing. Cloud could be seen as making it possible for users to tap into a supply of computing resource rather than manage the equipment needed to generate it themselves, much in the same way as consumers tapping into the national electricity supply instead of running their own generator.

However, for the time being, regulators have largely decided to consider cloud computing as outsourcing, subject to regulations already in existence for that activity. The industry welcomes the EBA's recently released draft guidance on using cloud computing in financial services. We will be responding to that in due course. However, we would like to highlight that so long as outsourcing rules designed for a different paradigm remain the relevant regulatory consideration, the use of cloud in financial services will continue to suffer from unnecessary frictions.

> **Recommendation**: In the longer term, a fundamental review of outsourcing regulation is necessary to adjust for the new world of FinTech. From the point of view of the financial services industry, the jurisdiction that best achieves an approach to outsourcing regulation which enables cloud computing will have a significant completive advantage as a place to experiment, roll out new innovative services, and to base a business.

DLT

Distributed Ledger Technology (DLT) is a change in storage and processing technology and potentially impacts and improves a number of digital process in Financial Services (Payments, Securities Markets, Trade Finance, Insurance, etc.). Distributed ledgers provide a consistent and secure record of activity in and ownership of assets (from "cash" through complicated derivatives) at scale and facilitate process automation through Smart Contracts.

While DLT is still at an early stage of development and deployment, its potentially transformative implications raise important questions and considerations for policymakers, regulators and lawmakers as well as for financial services institutions and users. At the outset, we consider that there are some guiding principles which are helpful to keep in mind when assessing the legal and regulatory considerations relating to DLT. These are:

- *A flexible and pragmatic approach – a "one size fits all" regulatory approach for DLT is unlikely to be effective or proportionate given its numerous potential*
- *Regulate the specific application and not DLT*
- *Harmonised international approach*

If it would be helpful to your consideration, the BBA and PaymentsUK, soon to be UK Finance, would be happy to meet and discuss the points raised in this response.

Yours sincerely,

Matthew Field, Policy Advisor Digital (matthew.field@ukfinance.org.uk**)**
Rhiannon Butterfield, Head of Regulatory and Government Engagement
(rhiannon.butterfield@ukfinance.org.uk**)**

Executive Summary:

1. We are grateful for the opportunity to provide evidence and views at an early stage to help the European Commission (EC) consider how to make the European financial sector more competitive and innovative. We cover the issues below in the order they are addressed in the consultation.

2. We would like to emphasise that a number of technologies being deployed or researched in financial services are in fact evolutions of existing technology (Big Data) or combinations of other technologies, some new and some not (DLT, AI). As such, we strongly support the EC's stated principle of technology neutrality and specifically outcomes-based approach that allows for innovation to continue and the technologies involved to continue to evolve.

3. For the reasons we outline, we believe that automated advice has the potential to enhance financial inclusion. However, **we do not agree that enhanced oversight of the use of artificial intelligence is required nor do we think that minimum information standards should be set for use in algorithms.**

4. Regarding Big Data and robo-advice, we detail potential risks below, but we believe that those risks are best addressed through outcome-based regulation of the activity being performed rather than through regulation of Big Data or AI explicitly. We note both Big Data and AI are, in fact, combinations of different technologies. In general, we believe that the benefits that Big Data and AI can bring to consumers and markets beyond robo-advice deserve greater consideration by the EC.

5. There are examples of price differentiation and tiering which have long been the case in financial services. The existence of Big Data analytics means that this is occurring on a larger scale. However, it is important to note that it is not a new phenomenon caused by Big Data but rather the gradual evolution of the use of greater amounts of data in financial services.

6. Several examples of new technologies that can improve access to financial services are given below. We note in particular the potential for technology to improve the financial security of consumers through, for instance, nudge behaviours as well as the possibility that Digital ID combined with DLT may provide AML and KYC solutions.

7. There are a number of promising use cases for improving processes, but we draw the Commission's attention to **the need to make national e-ID systems interoperable between Member States** and with third countries and accessible for the private sector to verify the identity of customers at distance. Beyond that, we invite the Commission to pursue a consistent regulatory approach specifically in the area of **harmonisation of outsourcing requirements**.

8. The industry considers RegTech an area of immense potential to reduce costs and increase market integrity. We note particularly the role that Big Data analytics will play in potential solutions and **encourage European regulators to more actively encourage market participation in this area through the creation of a RegTech Regulatory Sandbox.**

9. Regarding cloud computing, variation of outsourcing rules across jurisdictions is currently one of the greatest hurdles to greater use of the technology in financial services. Although we welcome the EBA's recent draft guidelines, we believe that to truly address the problem **a more thorough review of outsourcing regulation to account for modern outsourcing practices including cloud computing will be required.** Ultimately the Commission should work to establish a consistent regulatory framework at a global level.

10. We regard DLT as having significant potential to disrupt current practices in financial services to the benefit of consumers and the market. We note in our response several implementation challenges including governance, privacy and identity management, key managements, reversibility and settlement finality. Under technology hurdles we note in particular the issues of scalability and interoperability. The industry is aware of these issues and continues to look for innovative solutions that will allow this still young technology to come to market.

11. We agree with ESMA that there are currently no identified major regulatory impediments within the EU framework to the use of DLT. We detail several principles that policy makers and regulators

should apply when considering DLT and note particularly that its potential uses are varied, thus **a "one size fits all" regulatory framework for DLT will not be effective or proportionate, and that any framework should focus on the application of DLT as opposed to its use.**

12. We describe some of the ways in which the current regulatory or supervisory framework governing outsourcing is an obstacle including the areas of reporting requirements and third-party liability. Eventually, as for cloud computing, **it will be necessary to move toward a harmonised approach to outsourcing technology in financial services**.

13. We detail in our response the ways in which legislation and supervisory practices need to be changed to encourage FinTech. In general, **firms require greater flexibility with how they manage the risks associated with the use of FinTech solutions.** We note here that facilitating greater collaboration between large firms and technology companies, whether large or small, will encourage the growth of an EU FinTech ecosystem. We recommend that **regulators work with industry associations to facilitate partnerships through a referral tool or service.** Regulators are increasingly in a unique position to see where there would be potential for partnerships to develop innovative solutions to market problems.

14. Our response provides evidence that partnerships between large firms and start-ups should not be seen as a barrier to the latter achieving scale. We further raise a number of points regarding a FinTech licence and **recommend that were the Commission to explore such a notion that they consult publicly on the design of any licence.**

15. **We strongly support any EU initiative that could remove restrictions to the free flow of data** which at the same time acknowledges the right that businesses have to choose where they store their own data. We also support the Commission's three principles including technology neutrality, which we regard as imperative given the use of technology in financial services is only going to increase in the coming years.

16. When it comes to role of supervisors in enabling innovation we **encourage the creation of a European-wide Regulatory Sandbox, if structured correctly, and recommend that regulators consult publicly on its design in order to utilise the deep industry experience working with various regulatory sandboxes around the world. We welcome a global approach to sandboxes to avoid un-level playing field and to facilitate successful innovations are implemented across Europe and non-EU jurisdictions with minimum delay**.

17. **We do not believe that the European System of Financial Supervision (ESFS) needs to play a more proactive role in the development of standards.** Instead, we believe that there are opportunities to promote global standards before considering jurisdiction based standards in a way that would support the objectives of the European Commission.

18. In chapter four we address, among other things, the implications of data protection law for DLT. We hold that DLT should be treated the same as any other technology in regards to personal data protection. We believe the existing legal and regulatory framework provides sufficient protection **thus regulators should not introduce requirements related to data protection for DLT solutions specifically.**

19. We conclude that **no additional cyber security requirements for financial service providers and market infrastructures should be included as a complement to the existing requirements.** We stress that effective cyber defence requires a global perspective. We thus **strongly support regulatory harmonisation by global supervisors around risk-based approaches to cyber security risk management.**

20. We must continue to improve collaboration between industry and regulators, and also collaboration among regulators, to make meaningful progress in effectively meeting the evolving threat posed by cyber attacks. To achieve this we point to the **need for the recently introduced exclusion for the prevention of fraud within GDPR to be extended to cyber security prevention and monitoring. We further recommend that a legal construct akin to the Joint Money Laundering Taskforce (JMLIT) is needed** to provide full legal cover to allow greater cyber security information sharing at

national and EU level. It is important that a legal framework is established for data sharing for resilience and risk mitigation purposes.

21. Finally, **we support firms conducting their own penetration testing** in partnership with the regulatory community. We note that currently **the variation of regulatory expectations across multiple jurisdictions is a barrier to EU level testing**. There may be opportunity for harmonisation of the testing of financial institutions and other FinTech companies.

Detailed response:

1.1 What type of FinTech applications do you use, how often and why? In which area of financial services would you like to see more FinTech solutions and why?

Banks use FinTech applications and/or technologies for a variety of purposes. This includes:

General services

- End-to-end digital banking – the ability to open an account and complete the majority of transactions on a mobile phone.
- Investment advice and self-directed investing – online vehicles for both individual retirement and non-retirement accounts, providing easy-to-use (and inexpensive) automated advice, as well as enabling customers to buy and sell stocks and bonds, etc. (again inexpensively).
- Electronic trading and other online services (e.g., cash management)
- consumer payment systems;
- mortgages;
- auto finance;
- wealth management;
- small business lending;
- communications systems
- compliance;
- cyber resiliency;
- and general IT operations

Financial inclusion

Technology can assist in managing income and expense volatility – e.g. automated savings tools that identify small amounts of money that can be moved into savings based on spending and income (according to one member, use of this technology has helped customers in America save more than $350million).

Cloud Technology

Internal/Private Cloud: the internal cloud provides developers with rapid agility, allowing for more time on developing as opposed to provisioning infrastructure and application services. Banks expect the number of applications hosted in such platforms to grow rapidly.

Public cloud: Public cloud reduces peak infrastructure requirements by providing compute services during temporary fluctuations in demand. Furthermore, it also helps reduce long-term storage costs and accelerates developer access to cloud services.

Application Programing Interfaces (APIs)

Internal API stores: these can provide access to a marketplace of secure application services to internal developers. The 'Old world' of developing and writing unique code is being replaced by reusable component pieces ("micro services") that can communicate seamlessly. This reduces integration development time and improves developer efficiency.

External API: Expanded APIs offered externally to enable direct client integration and secure solutions by third-party developers.

Data analytics / Big Data

New technologies are allowing banks to access and analyse data in ways that they could not have done previously. For example, one bank has re-engineered its market risk platform, which now manages over 1 billion risk sensitivities and provides visibility 17 times faster than the previous system while delivering a more granular and holistic view of the firms risk exposure.

Robotics / machine learning

Robotic automation software automates routine, repetitive activity that would otherwise be performed manually. Actual bots available 24/7 to efficiently execute simple processes

without the risk of human error – e.g. automating systems access administration, for which some banks expect to automate up to 2 million requests each in 2017 alone. Savings from robotic process automation will allow banks to position their workforces around higher-value tasks and functions.

Machine Learning: Machine learning technology provides insights about data without needing to pre-program algorithms, and actively learns from data with the goal of predicting outcomes. E.g. Contract intelligence platforms that use unsupervised machine learning to analyse legal documents and to extract important data points and clauses. In an initial implementation of this technology, one bank has been able to extract 150 relevant attributes from 12,000 annual commercial credit agreements in seconds compared with as many as 360,000 hours per year under manual review. This capability has far-reaching implications considering that approximately 80% of loan servicing errors today are due to contract interpretation errors. Machine learning could also be used to drive predictive recommendations for Investment Banking.

Cognitive automation: Cognitive automation, which combines both robotics and machine learning technologies to mimic human judgment. Cognitive automation has the potential to automate more complex, human-like processes, such as perceiving, hypothesizing and reasoning. E.g. Virtual assistant technology to respond to employee technology service desk requests through a natural language interface.

In terms of where banks would welcome FinTech solutions, these include areas such as Corporate and Investment Banking, IT core banking solutions, and solutions focused on enhancement of data quality and the data architecture. Unfortunately, in some cases, a deepening of cooperation with Fintech startups which could address some of these areas is constrained by certain regulations (e.g. the coexistence of 'profiling' or the right to erasure ('right to be forgotten') within the General Data Protection Regulation (GDPR), which can be an issue for the use of automated decision-making processes in the context of robo-advice. In addition, most solutions provided by technology companies large and small are developed on a cloud first basis. Removing barriers to the use of cloud computing in financial services (discussed in more detail in questions 2.2 and 2.5.1) is key to increasing the rate and degree of collaboration between banks and FinTech startups.

In addition, FinTech could potentially help to deliver more collaboration between larger consumer and b2b brands and financial institutions. Finance is usually a key component of larger customer questions – e.g. balances and payments as part of overall cash management for small businesses, affordability and budgeting for holidays for personal consumers. Fintech companies cover a range of areas and include account aggregation, customer insights, financial management tools for consumers and SME, pensions and saving tools.

The Banking sector is particularly interested in partnerships with firms proposing new capabilities rather than applications, e.g., technologies that would allow banks to validate new data sources for credit risk, rather than offering a specific credit risk model. That applies across the business areas of banks.

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.) and at what pace? Are these services better adapted to user needs? Please explain.

Banks have substantial experience providing detailed personalised financial planning services to the benefit of their customers. This is not only advice for investment, but also includes the use of technology and customer service to help customers in every financial situation – from financial distress to long-term planning.

Certain forms of automation in financial advice are already widely adopted and commonly accepted (e.g. providing online investment advice when a client purchases financial instruments online, having a customer completing a MiFID questionnaire online, having a

customer providing information needed to apply for a mortgage credit online etc.). Robo-advice is another step in this direction.

Improvements in data collection and analytics which we have come to know as Big Data are a natural evolution of the data-driven processes that the financial industry has long used to improve its understanding of consumers/customers in order to better serve them. Robo-advice typically combines a range of financial tools in order to, among other things, manage clients' investment portfolio and optimize it, based on the client's investment goals and risk appetite.

This continually evolving data-driven approach can be applied to and improve many processes that might typically rely on intuition or limited or incomplete information. While fully respecting privacy, and within the context of data privacy regulations, banks can make better use of this data through advanced analytics in order to enhance the customer experience, e.g. through:

- Creating products that connect savings and spending or help address mismatches between consumption and income patterns;
- Offering contextualised, targeted products and experiences;
- Making more accurate credit-worthiness assessments;
- Providing better financial advice;
- Reducing costs for consumers, and
- Better protecting customers from fraud.

Financial Inclusion:
In terms of evidence about whether automated financial advice reaches more customers, as banks have worked to improve their product offerings it has become clear that automated financial advice could result in significant consumer benefits including enabling greater financial inclusion and simplifying the investment process for mass market. For both investments and other financial advice, automation will bring services to client groups who previously had no access to it including customers with smaller savings. We consider this will particularly be the case when Robo-advice is employed by incumbent banks whose customer base allows them to reach a large number of customers. The benefits of robo-advice which allow this are:

1. Decreased price;
2. A wider range of choices in terms of services offered and customization capabilities;
3. Greater ubiquity/geographic scope of financial advice availability.

As the pace of technology change increases and customers correspondingly grow more comfortable using technology to conduct financial business we expect this area to experience sustained growth. Though of course the increased automation will not mean that customers will cease having the possibility for a personal contact with financial advisors. Banks will continue to cater for both the digital savvy and its traditional client demographics. Complex financial needs will still require access to human advisors to assess best approaches to financial structuring.

With Robo-advice remaining in the early stages of development, banks of all types, whether incumbent, challenger or digital only, are working to deploy this service within the framework of the relevant regulation which already governs financial advice and the use of personal data, MiFID and GDPR being the most relevant.

It is also important to note that the financial automated advices developed by banks focus mostly on the provision of information, comparison websites and calculators. A clear distinction should therefore be made between the use of an automated tool and the use of automated financial advice, and consequently also between MiFID and non-MiFID services (investment services should be regulated under MiFID but not the other types of services like comparison websites).

Finally, privacy and management of client identifying data remains a top priority for banks. Financial services use cases require implementation of the highest levels of confidentiality

for data handling / storage mechanisms. Often solutions that are well established in other industries – for example cloud storage – remain difficult to implement in practice in financial services. Nevertheless, banks and other financial institutions have long been custodians and users of data, and have well established systems and protocols for using and protecting sensitive data on a large scale in compliance with the applicable legal and regulatory requirements.

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? What could be effective alternatives to such a system?

NO

First, it must be remembered that (artificial intelligence) AI is still in its initial growth phase and the technology continues to develop and evolve on a near constant basis. We must also be clear that AI is an umbrella term to cover a confluence of multiple technologies, such as machine learning, which includes deep learning, cognitive computing, natural language processing, neural networks, etc. AI can be divided broadly into three stages: artificial narrow intelligence (ANI, intelligence restricted to one functional area), artificial general intelligence (AGI, includes powers of reasoning, problem-solving, abstract thinking) and artificial super intelligence (ASI, surpasses human intelligence in all fields).

AI is not solely a financial services issue and any action taken must be considered in the context of the development of the technology in other sectors. Considering that AI is in its infancy we believe that although the ethical, legal and societal impacts deserve scrutiny, premature action on this front could potentially result in a limit to the consumer and market benefits that the technology may bring. Rather than premature regulation, we would envisage an ongoing dialogue with regulators which would translate into alignment of supervisory experience. Given this we see regulating outcomes as the best approach in this area.

Before any action in this area could be taken, there are a number of regulations already inexistence that impact upon the working of AI which would need to be considered. The use of personal data of course already has regulatory oversight in a number of areas, for instance antitrust for pricing. Under the GDPR there is an obligation on data controllers around automated processing. This includes the need to understand the underlying algorithms in detail to provide customers with the logic behind that reasoning. Finally, there are further requirements under MiFID II which must also be considered in order to ensure regulatory alignment.

As with all models and algorithms, it is necessary to implement a robust framework for documentation, development, testing and maintenance of systems to ensure transparency and unintended consequences. Oversight is required from both a technology infrastructure and legal, risk and controls perspective. Failing to provide suitable oversight will ultimately lead to negative experiences for clients across the wealth continuum, particularly in a bear market where limitations of models are more likely to be exposed. Incumbent banks will have controls and oversight processes and procedures in place (albeit they may need refining to deal with AI models). Given the risks associated with handling and holding client assets, the right balance must be found between ensuring suitable oversight, controls and regulation while not stifling innovation.

Therefore, an effective way to guarantee transparency and control should be pursued, without sacrificing the notable and remarkable potentialities of this technology. In our view, the use of simulations is the best way of monitoring an AI system, rather than trying to read the reasoning in the AI algorithms. Such approaches are more likely to yield the desired result of ensuring a safe and fair financial services sector while not limiting the kind of innovation currently taking place that has the potential to improve both customer offerings

and the market, and whilst adhering to the principles of technology neutrality and outcomes-based regulation.

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)?

As noted in our answer to question 1.3, we do not believe that it is effective to focus on the details of the algorithms in use, but rather regulators should look at outcomes. We do not believe that a minimum information base should be considered for a number of reasons.

First, it is necessary to remember that assessment of the customer's risk profile cannot be entirely automated and requires supervision by experts within the banks. Second, the developing nature of Big Data, analytics and robo-advice (as one single use case among many for the underlying technologies) is too new to determine precisely what data is required. Theoretically, as the AI learns it may become clear that different (whether more or less) data points are required to provide the best possible service. As such, any effort to set a minimum amount or characteristics of information about the service user (across the whole industry) risks limiting the development of the technology and therefore possibly the benefit available to consumers. Thirdly, as other regulation relevant to the provision of financial advice or the use of data changes the relevant minimums could change with them. The regulations could then end up being inconsistent or even contradictory. In the case of financial advice this could have damaging consequences to consumers.

Finally, setting such minimum standards specifically for algorithms as opposed to the existing standards for financial advice could be considered regulation of technology and a violation of the principle of technology neutrality. We therefore recommend that automated financial advice be regulated according to outcomes. As it currently stands, services and regulation should rely on data that could allow practitioners (both startups and incumbents) to be compliant with existing regulation such as GDPR and financial markets regulation (e.g. suitability, KYC).

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?

As noted in our answer to question 1.2 we highlight that there are other applications for Big Data analytics and artificial intelligence than robo-advice. These use cases could have substantial positive effects on consumers and the market including in the areas of enhanced AML/KYC checking and the continued exploration into the use of Big Data to increase consumer access to credit. We maintain that the best approach to ensuring consumer protection is to regulate for the service and not the means by which this is provided.

Customer trust is vital to banks' business, requiring high levels of security and reliability. New uses of data are evaluated from the perspective of no harm to the customer and firm reputational risk review. With the ongoing development of new products come changes to the way consumers are accustomed to receiving financial advice. Some consumers will likely prefer to interaction with a human advisor, for example. As in many sectors, it is widely expected that the use of AI will allow existing customer representatives to concentrate on consumer service over the completion of mundane tasks.

Banks also consider customer service to be an area of intense competitive pressure and will therefore continue to attempt to provide a level of service that meets or exceeds customer expectations. Competition is likely to be an effective insurer of strong customer service. As we are currently seeing, the market for companies offering automated financial advice is increasingly competitive bringing greater choice for consumers and encouraging higher levels of customer service across the market.

With respect to consumer protection, the same levels can be applied to robo-advisory as with branch-based financial advice. Customers are provided with support via interaction with call centre staff via chat/call to answer questions and address concerns. Additionally, based on the customer feedback, it can be ensured that specific questions are monitored and added to a knowledge database or enhanced onboarding journey to help the customer.

The banking industry is aware of the potential for differential treatment of consumers, but believes this can be best mitigated with sound controls, including proper de-personalisation and aggregation of data, and appropriate human interpretation of findings and how to apply the findings to banking practices. The human interpretation should adopt the "no customer harm" review lens and should keep in mind the Unfair Commercial Practices and Unfair Contract Terms regulations.

It is difficult to anticipate the extent to which more risk-based credit scoring might limit credit to those who cannot afford it – this depends on the risk appetite of various financial institutions. Any decision not to extend credit would be taken in the context of sound risk management (involving human decisioning) and to further the goals of safety and stability. Additionally, the banking industry needs to ensure that when working within the artificial intelligence or Big Data space that their algorithms are fair and unbiased to ensure positive customer outcomes. The guiding principles of ethical standards should inform guide rails which will ensure risks are managed from the design stage. However, these risks can change and thus the algorithms underlying the technology and the principles guiding them may need to be adapted.

Considering that further evolution is expected in the use of Artificial Intelligence and Big Data, the banking sector is currently assessing their applicability and the deployment of technological developments as well as the impact of existing and recent legislations on innovations in this field. Indeed, several existing EU legislations and/or other regulatory requirements such as the Payment Services Directive 2, GDPR, the Markets in Financial Instruments Directive (MIFID 2), etc. are expected to mitigate potential risks which could be linked to the lack of transparency, misuse of data, consumers being "locked-in" etc. For example, MIFID II is expected to lead to important changes in the organisation of the consultancy services offered by banks to their customers, following introduction of the new rules on consultancy (investment advice), incentives (inducement) and suitability assessment.

We conclude that it is thus too early to fully assess the risks and the critical aspects in terms of investor/consumer protection which this new method of interaction will involve for investors/consumers. Further, existing regulation already provides a strong level of protection and will continue to do so as the greater use of data in banking evolves. Similar reasoning also applies to the definition of the legal liability of each actor involved in the given service (e.g. cognitive engine provider, system integrator that trained the machine, company offering the service, users themselves). As such, it could be argued that the best approach for ensuring consumer protection is for banks to take a risk based approach to mitigating and controlling for possible consumer protection risks. In time it is possible to imagine the certification of cognitive engines or the monitoring of training activities and the use of the applications.

1.6 Are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding? In what way? What are the critical components of those regimes?

Although different jurisdictions are at varying stages of regulation for crowdfunding capital raising (CCR), we would support an alignment of regional and international frameworks. For example, this could be the development of commonly-agreed principles for regulating all (bank and non-bank-aligned) CCR platforms, with the goal of promoting a level playing field and consistency across jurisdictions. These common regulatory principles could include, for example, agreed standards on issuing licenses to operate CCR platforms and a mutually-agreed code of conduct. Amongst other benefits, we believe that this could enhance trust between all connected parties, and thus work beneficially for the industry at large.

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?

No response

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?

No response

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?

Sensor based technology is being tested within the industry to deliver more personalised insurance needs across both retail and commercial sectors. These technologies can be used to build preventative propositions by alerting customers to risks or encouraging behaviours to reduce risk. However, these technologies are only in their infancy and the industry is alive to potential risks such as out-pricing vulnerable customers, particularly in the health insurance sector.

1.10 Are there already examples of price discrimination of users through the use of Big Data? Can you please provide examples of what are the criteria used to discriminate on price (e.g. sensor analytics, requests for information, etc.)?

In general, firms already tier or differentiate between clients based on information available. For example: (i) trading clients might be tiered A / B / C based on their relationship and business size, with each of these tiers receiving different pricing as well as a different level of service; or (ii) in the insurance industry where rates are set based on a number of factors such as gender and wealth bracket, amongst others. All of this requires data, and the use of Big Data analytics means that it is occurring at a larger scale. However, it is important to note that it is not a new phenomenon caused by Big Data. The possible risks of Big Data, and means by which those risks might be mitigated, have been addressed elsewhere in our response, including in Q1.5.

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?

In general, technology is reinventing the financial service landscape with more convenient, affordable products and services as well as a safer more competitive market. We are seeing new products developed, and new mechanisms of product and service delivery, that reach vulnerable consumers at scale.

Technologies which allow financial services to be subscribed to and activated remotely and via digital channels, or which make the purchasing process simple while still providing guarantees for the parties involved, are central to the innovation being pursued by banks. While some technological advancements may open products to whole new classes of customers (e.g. robo-advice discussed above), others may simply streamline existing processes making it easier for consumers to conduct their banking tasks. These should not be overlooked as more efficient and effective processes open opportunities for banks to innovate from which more significant improvements to the customer experience may develop.

There is also considerable potential in the use of technology to improve financial security for customers. Promising FinTech approaches are using behavioural science principles, such as reminders and commitment devices, to nudge people to make better decisions. FinTech has

also enabled products that include customized and action-oriented information, in contrast to generic financial information campaigns which are not as effective at producing behavioural change. Of course, technology alone will not address financial insecurity. To ensure the adoption and usage of FinTech products in some cases will require delivery through trusted intermediaries, such as non-profit and community partners. A good example which has been operational in the United States for some time is automated savings tools that can assist in managing income and expense volatility by identifying small amounts of money than can be moved into savings based on spending and income (in certain cases, this has helped Americans save more than $350million).

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) and could be considered as innovative, leading to new services. A smart contract can be defined as: pre-written logic or data models (computer code); stored and replicated on a distributed storage platform (a blockchain / distributed ledger); executed / run by a network of computers (usually the ones running the blockchain) or subset thereof; capable of making updates to the ledger. Blockchain and smart contracts have the potential to trigger far-reaching changes in banking processes.

Digital Identity: verifying and safeguarding identity has always been a core part of banking. We believe banks have the experience, expertise and infrastructure to help shape an open, cost-effective and widely accessible future platform for digital identity that could help to enhance access to financial services and products. This is not to say that we think banks should be the sole providers of identity platforms; quite the contrary. But as we work towards a digital identity future, banks can supply their expertise and infrastructure. The combination of digital identity and blockchain/DLT holds obvious potential in a number of areas of banking. Banks are keen to pursue with regulators potential AML and KYC solutions which could be enabled by this combination.

Other technologies that improve access to existing/ offer new services include e.g. chatbots – that make the interaction with the bank more accessible; and AI (new platforms are being developed for this to be put into e.g. messaging and voice platforms).

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?

Individual companies will best be able to speak to the innovations currently being explored in their firms. However, it is worth highlighting the sheer amount of research and experimentation underway in banks aimed at exploring the potential for FinTech solutions to improve processes and reduce costs. The expectation is that by doing so banks will ultimately be able to deliver better products to consumers and improve the financial services market.

As policy makers will no doubt be aware, much of this work is being done through collaboration both with startups offering new and innovative technology solutions, but also among the industry to explore ground breaking new infrastructures (discussed below). However, as the speed of technology change and innovation increases, it may not be enough for the industry to develop these solutions in isolation from regulators.

Some of the most promising use cases of FinTech to reduce costs and improve processes are:

<u>Distributed Ledger technology:</u>

DLT/blockchain could be a technology which assists the processes between parties that need to improve the information exchanged, particularly where no central dedicated infrastructures exist. DLT based technologies can also help banks streamline their processes and achieve substantial back-office cost savings. In the same way that SWIFT does, there are opportunities in financial services infrastructure for close collaboration to create economies of scale and

better processes through automation. There are a number of projects currently underway in which the various industry players cooperate on industry-wide solutions, these include consortia as well as looser alliances.

DLT Platforms

DLT comprises a combination of existing technologies, such as peer to peer networking, public key cryptography, hashing, distributed databases, consensus mechanisms, etc. For any given use case, firms may use some or all of the technologies that underpin DLT. Although we think it is too early to assess fully the challenges around DLT, the main challenge we see thus far is identifying compelling business cases around specific use cases, and at the same time having a network of participants with significant will to change. Gaining a critical mass of network participants is the biggest challenge to DLT adoption.

Thus far, industry participants have sought to address this obstacle by collaborating together in a number of ways, be it through consortia or less formal alliances. Such collaboration has led to the production of different platforms which may in turn be the route to market in the short to medium term for emerging DLT applications in the mainstream of financial services.

Regulators in other parts of the world have shown willingness to engage with these platforms which we view as a positive development. Regulatory involvement would be useful for the advancement of certain possible use cases including regulatory reporting.

Many DLT use case applications can provide regulatory reporting benefits. For example, regulators can be set up as 'supervisor nodes' on DLT networks, and then have sight of all transactions as they take place, removing the need for some 'after the event' MI reporting. Issues remain including the potential that organisations may be reluctant to offer complete access to regulators without first checking the data being given.

Smart Contracts can have regulatory rules built into them, providing obvious benefits. They can also be available to 'supervisor nodes' providing high levels of transparency. As above, risks remain including the potential that smart contract encoding contains bugs or code that results in unintended consequences which could then result in large numbers of automated transactions being executed incorrectly creating a situation in which recovery would be highly complex.

We thus encourage European regulators to begin considering the possibility of participating as a regulatory node on the various platforms and underlying ledgers currently in operation. We recognize the concerns that may be held around this potentiality and welcome the chance to explore the issue in further detail.

<u>E-ID:</u>

Client identification and verification and KYC checks represent costs to banks and insurance companies and considerable inconvenience to consumers. Currently consumers do not have the possibility to use biometrics, videocalls, third-party verification to verify their identity. A digital on-boarding process developed under the EU eIDAS Regulation that re-uses home state national digital ID schemes as well as other Member States' and equivalent non-EU countries' digital ID schemes would reduce costs, fraud and the time required to undertake KYC checks.

Recommendation: National e-ID systems should be made rapidly interoperable between Member States and with third countries and accessible for the private sector to verify the identity of customers at distance.

Privacy is of course paramount in this process and we understand that national authorities will prioritise this concern. However, we believe that in the long term a functioning E-ID system will increase, not decrease, privacy as it will allow consumers to maintain control of their own ID while sharing their information with those that they choose.

Other areas of interest are:

- robotics to reduce costs by re-framing existing processes to Enterpris-2-Enterprise processes;
- trading platforms that reduce costs while increasing markets transparency;
- robotics used to improve control by automating repetitive manual tasks with high rate of error and implemented with correct approach to operational risk;
- Use of advanced optical character recognition, voice recognition and other forms of developing AI;
- platforms used in Capital Markets to access data in a simpler and more efficient way;
- digitalisation of processes that facilitate the interaction with customers;
- AI/Big data use to better focus resources and sales on the right customers at the right time (which customer needs which product at which period of their life);
- robo-advisory to leverage sales in retail with better/more sophisticated products by low costs.

Please also revisit our answer to question 1.1. where several other FinTech applications like cloud computing, robotics and machine learning are discussed.

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?

Industry standards, defined Best Practice and third-party certification.
As discussed in the recent EBA consultation on Guidelines for ICT Risk under SREP, the creation of a harmonized global technology risk framework could be beneficial in removing or limiting many of these frictions caused by regulatory uncertainty. However, such a solution would need to be wide ranging and led by the industry itself in order to overcome the difficulties inherent in cross-jurisdictional approaches.

Where meaningful benefit could be achieved is in the recognition by EU regulators of defined best practice, industry standards or third party certifications in a range of technology areas. The industry stands ready to work with regulators on these solutions in order to ensure the safe and successful digitization of banking.

A number of factors support the use of defined best practice, industry standards or third party certifications:

- First, the industry has a clear motivation and has shown significant ability to mobilize swiftly when it comes to working together toward innovations that benefit consumers and markets;
- Second, the nature of many of the solutions being proposed require a high degree of cross-industry collaboration which makes industry standards, best practice or third party certification a natural method for ensuring secure and compliant technology change;
- Third, the speed of technology change is such that regulators risk hindering the development and deployment of innovations which could benefit consumers and strengthen markets by not allowing the industry, both banks and technology providers large and small, to work together to find ways to ensure solutions are both safe for consumers and markets and compliant with regulation.

We believe that close collaboration between regulators and industry in this regards presents a real opportunity to streamline innovation and benefit consumers and markets. The industry welcomes the chance to explore the potential of such solutions in greater detail.

Consistent regulatory approach:
Our general principle is that there should be a fair and level playing field and that certain activities should carry the same regulatory obligations regardless of who is carrying them out. Some new disruptive business models are in some cases challenging the current regulatory environment. It is thus highly important for policy makers to understand the functioning of these new technical applications, as well as their social, economic and regulatory implications. Although while on a small scale the risk is limited, there is genuine concern over the systemic risk posed by an increasing number of firms operating regulated activities while outside of the regulatory purview.

We encourage regulators to consider the balance necessary between enabling innovation and encouraging competition with preserving trust and security. An example is the area of KYC, AML and terrorist financing where trust in the industry more broadly could be damaged, thus potentially generating systemic risk, by the activities of the numerous non-banks which are now moving significant amounts of money between jurisdictions.

Cloud computing:
This is an area where the EU could play a substantial role in creating a more friendly environment for technology change and the use of FinTech solutions. We have gone into some detail in the introduction to this response. We lay out again what we consider to be the key areas where action is needed**.**

- **Adjusting the regulatory environment to the digital reality:** we observe that the legal and regulatory environment constrains somewhat the adoption of cloud service models by the banking industry. These constraints also create significant frictions in ensuring that regulatory compliance is achieved in contractual negotiations between banks and cloud service providers (CSPs).

- **Further harmonising regulatory approaches across different jurisdictions**. The variation in approaches to cloud computing in financial services by various national regulators creates inefficiencies, particularly for banks operating with a global presence and global customers. The uncertainty created by the variation in approach reduces the appeal of the EU as a place to do business. This is a challenge impacting business operating across financial services whether traditional banks or new startups; many of the new startups and neo-digital banks operating in the market are cloud native and will experience barriers to growth as a result of the lack of harmonisation across the EU. Finally, harmonising approaches to the cloud across jurisdictions will also help to facilitate the adoption of cloud at a global level which creates efficiencies and encourages growth.

- **The need for proportionality in cloud outsourcing requirements.** In order to successfully encourage firms to take advantage of the potential in cloud computing, relevant outsourcing requirements should be made proportionate to the risks incurred to the user in contracting to a CSP. Thus far, a limiting factor in achieving assurance arrangements in contracts is the costs to both users and CSPs in fulfilling outsourcing requirements.

- **Review outsourcing requirements**. More fundamentally, outsourcing requirements need to be assessed and updated to be made more relevant to the modern technology enabled world of finance. Arrangements for contracted cloud services often present different circumstances to traditional IT outsourcing. Certain cloud models are more akin to a utility than outsourcing. Cloud could be seen as making it possible for users to tap into a supply of computing resource rather than manage the equipment needed to generate it themselves, much in the same way as consumers tapping into the national electricity supply instead of running their own generator. Further, the wide range of possible cloud models and uses mean that firms face an equally wide variation in the level of risk they incur in using the 'cloud'. It is thus prohibitively difficult for users to adapt the legacy regulations around outsourcing to their cloud arrangements. Clear guidance for outsourcing to cloud service providers in financial services like that recently issued by the EBA based on proportionality may go some way toward encouraging the adoption of the

'cloud' by firms, but this will only be partially effective so long as the outsourcing regulation for which it is providing guidance is not written to address cloud services explicitly. The BBA welcomes the EBA's recently released draft guidance on using cloud computing in financial services and would urge the Commission to take note of our forthcoming response.

Recommendation: In the longer term, a fundamental review of outsourcing regulation is necessary to adjust for the new world of FinTech. From the point of view of the financial services industry, the jurisdiction that best achieves an approach to outsourcing regulation which enables cloud computing will have a significant completive advantage as a place to experiment, roll out new innovative services, and to base a business.

Digital financial education:
We see a role for the national governments, the European Commission, and relevant international bodies (such as IOSCO and the OECD), in coordinating national initiatives (or creating an EU framework) for increasing digital and financial literacy to enable consumers to operate efficiently in the digital environment and help them with making informed choices about their investments, and managing their online identities. These efforts would also feed into the wider objective of a broader and more equitable access to financial services and skill development. Ultimately it will foster a positive change in savings and spending habits. Finally, as digitalisation is one of the most fundamental structural changes we are going through. One way to strengthen the emerging ecosystems would be to focus on university education and research that would support a deep talent pool for financial services and expertise to grow business within Europe and beyond.

European Innovation Space:
We also believe that the acceleration of the benefits of digitisation and automation of financial advice for European consumers can be helped through a concerted regulatory effort to create a unified innovation space (e.g. the Roboadvisory work firms are currently undertaking in the UK in close collaboration with the FCA, but also similar work by other regulators such as the Money Advice Service, the Hong Kong Money Authority), which allows all actors in the market (incl. FinTech companies) to cooperate in exploring new innovations, shorten the time-to-market and to roll out those innovations for a broader customer base across country borders, including to non-EU countries that are also at the forefront of digital innovation (e.g. Switzerland).

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?

Automation and innovation do not necessarily mean a reduction in employment. Digitalisation is expected to create demand for new skills and competences, and may allow for the workforce to be positioned around higher-value tasks and functions. Having said this, we should acknowledge that technology will cause some disruption to jobs, and the emphasis should be put on digital skills and retraining. Firms in the financial industry will face the challenge to offer new creative jobs for employees (i.e. more qualified employees, attracting new talents and re-skilling existing employees). Furthermore, collaborating with FinTech businesses will help to enhance open mindedness, adaptability, fast execution, long term thinking, and new working methodologies (e.g. design thinking, Scrum, Agile, data science, business development, IT, and user experience). We expect that employees with specific competences on ICT, science, technology, engineering and mathematics are likely to be required.

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?

One of the most interesting areas of development that holds great possibilities to reduce costs and increase market safety is RegTech. RegTech has the potential to transform the

way financial institutions manage the regulatory environment, allowing them to be more efficient and dynamic in their response to new requirements and expectations. RegTech solutions could also free capital which can be put to more productive uses, increase competition by removing barriers to entry, improve the quality and efficiency of supervision, and reduce risk.

The IIF's report “Regtech in financial services: Technology solutions for compliance and reporting” identified areas that would benefit from RegTech, including risk data aggregation, modelling, forecasting, KYC, monitoring culture/behavior and trading surveillance and compliance. Yet, by its very nature, the involvement of not only the wider industry but regulators is required in order to make true progress in RegTech possible. RegTech providers are in need of shared access to multiple financial institutions to get a holistic picture of data such as client data, which provides greater visibility towards client transactions in cases like AML. This can be simplified with more secure cloud storage and cloud solutions, which can be shared by RegTech vendors and banks. EU and regional positioning of such cloud data centres can enable these functions across the financial institutions to perform and monitor effectively. The RegTech and cloud vendors are also finding this challenging to establish across geographical boundaries.

> **Recommendation: RegTech regulatory sandbox:** Regulators should actively explore how to encourage market players to develop RegTech solutions. This should include taking a more proactive approach to facilitating innovation in the financial services sector, particularly in the area of RegTech. At a minimum, this means an expertise build-up and creating forums for open discussion of RegTech/FinTech issues. A possible method is to use a regulatory sandbox to invite collaboration between market players and regulators. We believe this will require not only coordination across the industry, but a commitment from regulators to be actively involved in exploring solutions. Further, any sandbox must be empowered to meaningfully reduce regulatory requirements in order to increase the level of innovation already underway. Sandbox-like partnerships encourage innovation, allowing regulators to closely monitor a RegTech or FinTech firm’s operations in a limited-scale and safe regulatory environment.

The most promising use cases around RegTech are:

- automating otherwise manual processes. For example, horizon scanning and regulatory reporting tools can reduce workload within compliance teams.
- Know Your Customer/Ultimate Beneficial Ownership 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
- Anti-Money Laundering/Counterfeiting the Financing of Terrorism.

Data has become an integral part of compliance and regulatory affairs, which is empowered by the ability to understand and interpret data in the right way, but has always been a challenge for every organization. Interpreting data in the right way implies many things including making use of enterprise level data which can give actionable analytics, not having dark data (data which is collected and has significant impact, but is not used by IT systems) and having capabilities to understand, recognize patterns and learn as we analyse the data.

There is also a growing number of Reg-Tech solutions focused on the application of data analytics and so-called “Big Data.” These techniques can be used to reduce compliance risks in areas such as anti-money laundering. Big data techniques can identify potentially high risk customers (possibly in combination with biometrics to identify a client in a digital environment and/or authenticate a high risk transaction); make reporting information more accessible and easily searchable to regulators; improve internal culture and behaviour by better identifying actions that could lead to compliance violations or incur reputational risks to the institution; and in combining Big Data with artificial intelligence, allowing firms to reduce market risk through more precise modelling and forecasting of market trends and sentiments. Control and evaluation can be done more effectively via AI in the future. Using

robots (virtual, but also physical ones) can improve quality and also quantity of regulatory control and as a result lower risks.

2.5.1 What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services? Does this warrant measures at EU level?

In addition to the earlier comments in question 2.2 on outsourcing, there are a number of other obstacles preventing financial services firms from using cloud computing services.

Requirements under GDPR raise risks in relation to personal data. In particular, data controllers need to fully understand and be accountable for the data and associated risks (cross border, data flows to subcontracted third parties etc) when they use the services of cloud vendors. Regulation without a full understanding of the impacts may hinder innovation in this area. This is a significant barrier for banks entering wholesale into the cloud and is likely to inhibit the use of FinTech companies that offer innovative cloud solutions.

As discussed above, regulatory guidance on the use of cloud in financial services is necessary to bring certainty to institutions looking to use cloud. Such guidance will help banks qualify their risks and build viable cloud strategies. The EU should also consider how to help facilitate the conditions which allow the insurance industry to offer products in this area. The use of insurance mechanisms would encourage financial organisations to enter use cloud services on a larger scale.

The adoption of cloud services by the banking industry is hindered by various legal and regulatory requirements, as well as compliance requirements related to the use, management and storage of customer information. These requirements also create significant frictions in ensuring that regulatory compliance is achieved in contractual negotiations between banks and cloud service providers (CSPs).

Another key factor slowing down cloud adoption in Europe is the **lack of harmonisation in regulatory approaches across different jurisdictions.** The variation in approach to cloud computing in financial services by various national regulators creates inefficiencies, particularly for banks operating with a global presence and global customers. The uncertainty created by the variation in approach reduces the appeal of the EU as a place to do business. This is not unique to the incumbent banking industry. New FinTech start-ups, and neo-digital challenger banks, many of whom are cloud native, will experience barriers to growth as a result of the lack of policy harmonisation across the EU. Finally, harmonising approaches to the cloud across jurisdictions will also help to facilitate the adoption of cloud at a global level which creates efficiencies and encourages growth.

In addition, we observe that one of the hindrances to a consistent European Union (EU) and Global regulatory framework for Cloud Computing in Financial Services is related to regulation and domestic laws which establish **barriers to the geographic location of the physical Cloud Computing infrastructure**. Frictions to leveraging the benefits of Cloud Computing in Financial Services arise when data regimes restrict cross-border data flows, both within the EU and globally. Data stored in a Cloud Computing environment can be fragmented geographically and its support functions (such as processing, hosting, backup, support and management), divided among suppliers (often across national boundaries) to enhance their data security, disaster recovery and resilience. In this regard, this progress in technology towards a 'distributed' network infrastructure challenges traditional data and outsourcing concepts such as physical data localisation and auditing of physical premises.

According to the financial rules on outsourcing for many EU countries, financial institutions must notify the supervisor and obtain their approval to launch cloud projects. This notification and approval has to be done on a case by case basis. It implies an indirect constraint to the free flow of data and, thus, to a faster innovation and a more agile cloud adoption. There is a need to harmonize EU financial supervisors' criteria when approving cloud projects.

Prescriptive regulations on data localisation are at odds with trends in technology. The latter, unlimited by geographic boundaries can manage storage and access to data, located globally. In order to support and facilitate a responsible adoption of cloud computing within the banking industry, the European Commission should focus on efforts that support the **creation of a clear and consistent regulatory framework at an EU and Global level**, and guarantee a proportionate risk-based approach to due diligence and contracts between the Cloud Servicing Providers (CSPs) and the banking sector in respect of Cloud Computing in Financial Services.

2.5.2 Does this warrant measures at EU level?

(Yes/No/Don't Know- 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.

YES

We welcome the EBA's consultation on guidelines for outsourcing to CSPs in financial services as a good first step toward greater harmonisation.

The Commission should also continue its positive work under its Free Flow of Data Initiative to remove unnecessary data localisation requirements, except where necessary for legitimate public interest reasons.

Any EU initiative that could remove restrictions to the free flow of data while acknowledging the right that businesses have to choose where they store their own data, within reasonable regulatory safeguards to protect customer data privacy and minimize potential impacts through data loss, should be strongly encouraged. Companies' decisions on data localisation may be part of a specific business model and companies must be allowed to request or provide data localisation. This is a choice made by both providers and recipients of the service, which is quite different from a legislative obligation to do so.

2.6.1 Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with? Should commercially available cloud solutions include any specific contractual obligations to this end?

The quality of the product offering in terms of compliance with FS regulations varies between service providers. Some of the more mature service providers have made progress in offering terms which enable financial services firms to comply with the applicable regulatory / supervisory framework. However, other service providers still fail to accommodate these requirements. Overall, financial services firms continue to have difficulty in finding cloud based solutions that enable them to clearly comply with the applicable regulatory / supervisory framework.

Uncertainties pertaining to compliance with certain regulatory requirements, such as outsourcing requirements regarding effective supervision and oversight of CSPs and supply chains, challenge a proportionate risk-based approach to due diligence. The EBA's recently released draft guidance may go some way to mitigating these difficulties.

Banks currently go to great lengths to ensure regulatory compliance which can involve significant contractual difficulties with CSPs. This involves, among other things:

- having internal controls in place which achieve effective identification, monitoring and reporting of risk in terms of data protection, business continuity, etc;
- undertaking initial and ongoing due diligence of the CSP, but also of those service providers within the supply chain;
- ensuring that the arrangement with the CSP does not materially impair their ability to comply with the supervisory requirements or the ability of a regulator to monitor a bank's compliance with its regulatory obligations;

- taking steps to demonstrate that a regulator can exercise a right of effective access to data and to the business premises of service providers processing that data (more on which below);

More broadly, banks must demonstrate that they are using CSPs that commit to cooperating with regulators in connection with the oversight of the cloud arrangement. The extensive commitments required from the CSP create additional difficulties for banks.

Other concerns are that it becomes incredibly difficult to switch CSP. Contractual conditions are often not transferable because of the bespoke nature of the agreement and this is especially true as it pertains to adapting the contract to a different country of use. Thus banks must deal with a vendor lock-in situation which is unacceptable from a compliance and contractual point of view.

The second major concern is that owing to the extensive requirements, only a very limited number of CSPs are able to provide a service that allows banks to comply with regulatory frameworks. This creates a worry about concentration risk with the potential that a small number of cloud service providers could become systemically important. Banks are unable to monitor this situation and can only be concerned with ensuring that their own operations are not concentrated in too few CSPs. A corollary concern is that competition in the cloud service market is limited and small providers are unable to compete in their product offerings.

> **Recommendation:** There is a need to enable switching between cloud services. This can partially be achieved on a technical level through standardisation of API`s among CSP's which will help provide portability and prevent lock-in which is also critical for GDPR. The EC could drive this standardization work in collaboration with CSP's and Financial Service Companies. However, we note there remain additional commercial and legal hurdles preventing true interoperability and nor would we wish to remove the competitive nature of cloud service provision.

On the specific issue of auditing a service outsourced to the cloud, banks are required to cooperate with regulators, and generally secure (on-site) access rights to records, premises and personnel. Physical access to premises hosting the cloud infrastructure is often a point of tension in negotiations with CSPs, who may be reluctant to allow customers into their data centres for legitimate security and confidentiality reasons. Furthermore, in a globalised and distributed cloud model, access to the physical location delivers a negligible outcome, other than the most basic one of physical security and access checks. In contrast, a virtual audit of data can be of much greater relevance to ensuring appropriate controls are in place.

Complex supply chains such as a SaaS solution built on another provider's infrastructure/platform also make securing rights to have access / to interview personnel (for each party of the supply chain) challenging in negotiations. This challenge is further driven by an ambiguity concerning how far auditing rights should be exercised throughout the supply chain. Without clarity concerning what is required to comply with the regulatory framework, banks may either look to secure rights extensively all the way down the supply chain, or may, on the other hand, be forced to take on additional risk in not securing extensive audit rights.

The challenge for cloud providers is compounded by the large number of customers and by the standardised nature of their product offering which leads to a high level of complexity when giving individual customers the right to audit. As a result, effective identification, monitoring and reporting of risk is more difficult in many cloud environments given the lack of visibility in the whole supply chain of the technology stack.

A significant solution would be the production of EU wide guidance for the use of cloud computing in financial services such as that recently released by the EBA. The goal of such guidance should be to facilitate compliance by creating a commonly understood set of minimum requirements to operate in Europe. We thus encourage the Commission to consider closely the results of the EBA consultation due in August.

2.6.2 Should commercially available cloud solutions include any specific contractual obligations to this end?
(Yes/No/Don't Know- not relevant)
Please elaborate on your reply to whether commercially available cloud solutions should include any specific contractual obligations to this end.

Yes. See response 2.6.1.

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

We agree with the list of the potential applications of DLT in the FS sector listed on page 11-12 of the EC FinTech Consultation. There are numerous other potential applications that have been widely publicised, for example, cross-border Trade Finance, Supply Chain Finance, Identity Management, KYC, Bank Reference Data etc.

Regarding access to finance for SMEs, we do not think that DLT itself will meet the objectives of enhancing access to finance for enterprises. However, DLT may well result in disruptive changes to some of these business models that will meet the desired outcome. The underlying technology may include DLT, or selected parts of DLT to enable these business model changes.

The use of DLT may result in this kind of beneficial disruption either directly or indirectly:

- Directly - (local and cross-border) invoice financing – this could grow exponentially once the financed invoices are identified/ marked over a DL (when coupled with counterparty identity and credit risk attached to the invoice), and would also be trading in a secondary market.
- Indirectly – due to streamlined/ improved financial reporting, covenants monitoring and securities issuance over a DL. Examples include equity funding and dynamic/unsecured credit.

Disruption in any of these specific areas could result in enhancing access to finance for enterprises. This disruption is not limited to DLT, though DLT has been a catalyst for re-thinking many of these existing business models. In addition, the model of a distributed database can provide a single source of information where SMEs can share their financial data (assuming compliance with regulation, especially GDPR can be established) in order to help financial institutions to better assess their credit risk. This could make it easier for SMEs access to some banking services and especially financing services.

It could materialise via "Smart Contracts" – Blockchain functionality to execute pre-determined commands. In trade-finance and in invoice prepayments there are interesting applications supporting companies and SMEs.

Below are two examples of work underway. We would note that these activities and solutions often require collaboration across industry. There may be yet further gains to be made in the area of RegTech.

Utility Settlement Coin: A number of banks have been working on the concept of the Utility Settlement Coin (USC), an asset-backed digital cash instrument implemented on distributed ledger technology for use within global institutional financial markets. USC would be a series of cash assets, with a version for each of the major currencies (USD, EUR, GBP, CHF, etc.) and would be convertible at parity with a bank deposit in the corresponding currency. Unlike cash held as a commercial bank deposit, USC would be fully backed by cash assets held at a central bank. Essentially, spending a USC would be spending its paired real-world currency. The roll-out of the Utility Settlement Coin would basically mean the introduction of a common unit of value across different blockchain platforms in institutional markets. USC could have a

wide range benefits from balance sheet implications to improved processes around clearing and settlement. Through having a digital cash instrument, linked to central bank money, the risk, complexity and time taken to settle and clear trades could be significantly reduced.

Real time cross-border payments: Today banks rely on a network of correspondent banks that allow clients to make cross-border payments on an average of a T+1 / T+2 basis (though this time period can extend depending on the location of the payee and any additional checks and compliance that must be undertaken). A number of banks have been reviewing new blockchain-based payment protocols available on the market like Ripple and experimenting with a proof of concept platform based on Ethereum. These solutions take advantage of the capabilities of blockchain to execute payment obligations netting and enable real-time clearing without the involvement of correspondent banks on each transaction.

Other examples of possible DLT applications include supply chain finance and trade finance.

2.8 What are the main challenges for the implementation of DLT solutions (e.g. technological challenges, data standardisation and interoperability of DLT systems)?

On the technology side, we think that data and protocol standardisation, security and error recovery will be challenges. The nature of DLT, means that DLT errors will be common to all participants at the same time, as the ledger errors are synchronised to all participants. This highlights potential risks around Governance of a DLT network, such as membership criteria, membership vetting, certification, consensus mechanisms, certificate authority, standards ownership, identity management and supervisory participation.

It is important to identify some of the issues that the nascent technology will have to face and resolve before being considered as mature. This includes looking both at the governance and technological needs.

Governance and privacy needs:

- **Governance framework**. The DLT that is likely to be applied to financial services would be 'permission-based' in contrast to a 'permissionless' system (like Bitcoin) due to efficiency, security and privacy reasons. A permission-based framework requires rules to approve/reject authorised participants, including perhaps minimum capital requirements, conduct of business rules and risk management processes. In addition, rules to govern the interactions between participants, both 'permissioned' and 'non-permissioned' will be necessary. Examples include the liabilities of the respective participants, including in case of fraud or error, correction mechanisms and penalties in case of infringement to the rules, the intellectual property attached to the technology or the territoriality of the law likely to apply to the network. An agreement between the participants on their remuneration model would also be needed. Furthermore, the governance framework should provide clarity on the entity or group of entities that would be held liable for the activities of the network vis-à-vis third parties, in particular local regulators and customers.

- **Privacy management**. As currently designed all the distributed ledger networks (e.g. the Bitcoin Blockchain, Ripple, Ethereum, etc.) and their derivatives are fully open whereby any person/entity with an access to the network can see all account balances and the transactional behaviour of all participants. This is true for both the publicly available versions of these networks and for the private forks of the same networks that financial institutions may choose to run among themselves. Banks' customers (and the banks themselves) require their financial data to be private. The lack of privacy poses a problem whereby one financial institution may be able to monitor the transaction flows of another institution perhaps to gain some competitive advantage. Various solutions to the privacy issue exist. Some also address the issue in a manner that would be key for any regulatory reporting use case, whereby regulator nodes exist on enterprise DLT networks and have real-time transparency into market activity for reporting purposes, while maintaining appropriate privacy across the platform.

- **Identity management**. Whether for AML, KYC or simply being certain of the person/entity with whom parties are transacting, the identity of the participants in a distributed network needs to be assured. With certain distributed ledger-based protocols, identity does not matter; as long as the person at the other side of the transaction holds the necessary secret key that is all that is required to engage in a transaction. The same can be said for the transaction validators (miners), whose identity and location does not matter. Within the context of the financial industry, however, identity matters. It matters that financial institutions know who their customers are, it matters that the regulators know who the financial institutions are and it matters that the financial institutions know who the transaction validators are, and which ones they should trust. It also matters in which jurisdiction the transaction validators are located. The criteria for admittance to any trusted pool of transaction validators need to be carefully considered by the financial industry. Banks need to be certain of the identities of their customers and of the other banks with whom they transact. In a world where simple possession of a secret key can control access to funds, it is imperative to know exactly who controls those keys. Participants in a network, possibly including regulators, will need to determine some appropriate framework that offers guidance on how identity should be handled. Participants may also require some technical means to exclude certain transaction validators that are not compliant with certain laws or are exhibiting bad behaviour (however that may be defined).

One solution for addressing the issue of privacy would be so called 'self-sovereign identity' - one in which individuals own and control all of their own identity data. In such a self-sovereign identity platform, the individual takes on the role of identity provider, collecting all of his or her available attestations and attributes, and keeping them in a digital vault or other system (similar to the way we keep our passports and birth certificates at home in safe places). Through cryptographic means, for example, we can safely store and share attestations while ensuring that they can't be falsified or misused. We believe such a solution holds much promise. It offers optimal levels of privacy and security, and, as long as the surrounding ecosystem is geared towards it, would offer individuals almost complete control over their identity data and personas. Such a decentralized system may also be the only solution that can stand up to the long term stresses to which any global and increasingly complex identity system is likely to be subjected.

- **Key Management**. Cryptographic keys are somewhat analogous to passwords. For security purposes they will need to be changed regularly. A fundamental property of distributed ledgers is that the activities of any particular account (address, wallet, etc.) is controlled by some private cryptographic key (or combination of keys) that gives the holder of that key the ability to digitally sign a transaction so that the counterparty to that transaction can be completely sure that only the person with the correct secret key could indeed perform that transaction. The problem with secret keys is that if a nefarious actor manages to uncover (hack, steal, etc.) the necessary secret key (or combination of keys), malicious transactions become a real possibility. Most systems also provide multi-signature functionality in that some "m" of "n" keys may be required to effect a transaction and each key could possibly be assigned a different weight for importance. In practice this feature could be used where financial institution's legal department, operations, and IT department might all be required to digitally sign a transaction before the transaction is irreversibly processed. The industry/participants would need to determine best practice on how often a financial institution should change its keys and how those keys should be stored (online, offline, hardware, etc.).

- **Reversibility**. To correct mistakes and fraud, banks require ways to reverse certain transactions. One of the key features of distributed ledgers is that once a transaction is digitally signed it is irreversible from a technical point of view. In the real world financial institutions do make mistakes. When transactions are irreversible there is a significant risk that funds that are sent in error or due to theft or fraud may never be recovered. For distributed networks to be useable by financial institutions, the banks and their clients need to have some assurance that they have some recourse in case

of mistakes or worse. Again, participants or the industry more widely will need to determine best practice for reversibility to be ensured in the case of error or fraud. There is also the possibility of requiring some kind of freezing mechanism should digital funds end up in the wrong hands. From a technical point-of-view there are some good solutions available, but there remain legal questions around the mechanism of freezing and what happens to frozen funds.

- **Settlement Finality**. When funds and assets change hands, there is a point at which the transaction is considered legally settled. With distributed ledgers, assets are represented as digital tokens and the ownership of an appropriate secret key gives the key holder control over those tokens. With Bitcoin, the movement of tokens in a transaction represents settlement of that transaction. I.e. the tokens are effectively digital bearer assets. The key question for financial institutions and the legal community to answer is whether mere control of digital tokens represents actual ownership of what they represent in the real world or if those tokens are merely representations of some obligation of a real-world counterparty that would at some time in the future have to perform against those obligations (i.e. are the tokens IOU's or are they actually digital assets?). This question is most important when it comes to tokens that represent fiat currency because the problem arises that a token issued by one financial institution may not be valued the same as a token issued by another financial institution (i.e. EUR.bank1 may not be valued 1:1 against EUR.bank2). In other words, the differing values of the same currency IOU's from differing issuers becomes a problem. In the first case (tokenized asset), much legal and regulatory work remains to be done regarding the nature of those tokens. And even once this work is done, the interpretation of such legal frameworks may vary from one jurisdiction to another (highlighting the need for a cross-jurisdictional approach to standards and regulation). In the second case (differing values of the same-currency IOU's or 'settlement coin') one solution is to propose that a central bank directly issues digital tokens (either to banks or to consumers) that represent its own currency and for those tokens to be treated in much the same way as cash is today. There are many additional benefits to this approach including fine grained control over monetary policy.

Technological needs

- **Scalability**: Scalability is recognized by industry as a challenge for DLT. Thus we have seen research and development continues on the issue, and believe that it will be solved over time.

- **Interoperability**: As DLT will probably be used firstly in niche applications, they would need to interoperate with existing infrastructures. Also, there will be different ledgers for different asset types (or even industries) that will need to interact with one another. Interoperability will also become crucial in case of the existence of several ledgers where two parallel (e.g. intentionally malicious) transactions with the same asset could potentially be executed. A question in this case relates to which transaction has to be considered valid / legal. There are technical challenges that can only be relieved by the adoption of common standards by all the players in the field.

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 for question 2.8 above, regulatory challenges are more applicable to individual use cases rather than the underlying technology.

We share the ESMA view and have currently not identified major impediments in the EU regulatory framework that would prevent the emergence of DLT in the short term. We also fully support ESMA's view that any regulatory or supervisory action for DLT would be premature in the short term. At this stage, a cautious approach to regulating DLT is advisable, since it is not completely clear yet what the impact of these technologies on banks' services

or what the potential regulatory obstacles will be. Having said this, as policymakers continue to consider DLT within the context of the regulatory and supervisory framework the following should be taken into account:

- The potential uses for DLT are numerous and diverse. Consequently, the adoption of a "one size fits all" regulatory framework for DLT will not be effective.
- If a situation arises where the use of DLT poses challenges within a certain regulation, policymakers should take a pragmatic approach to such situations. The possibility of DLT not fitting within certain regulations should not be viewed negatively, given that the current regulatory framework was not written to accommodate a technology like DLT.
- Regulate the specific application, not DLT: while there may be aspects of the regulatory framework relevant to DLT as a technology platform, this is distinct from applying a regulatory framework to regulated financial activity that utilizes DLT.
- Divergent regulatory approaches to DLT in different jurisdictions may hinder the adoption of DLT in an optimally beneficial way. To this extent, we would urge regulatory cooperation and international harmonisation to enable an effective and facilitative DLT framework.

Furthermore, we also share ESMA's opinion that a number of concepts or principles (e.g. the legal certainty attached to DLT records or settlement finality) may require clarification. As ESMA correctly realizes, beyond pure financial regulation, broader legal issues, such as corporate law, contract law, insolvency law or competition law, may impact on the deployment of DLT.

In particular, we believe that with further development of the technology, the following regulatory issues might need to be addressed:

- The legal framework regarding the nature of blockchains and distributed ledgers (DLs) in general, including territoriality (jurisdiction issues and applicable law) and liability (responsibility when something goes wrong).
- The legal framework for the recognition of DLs as immutable, tamper-proof sources of truth regarding the information stored on it. Related to this, the legal frameworks for the use of DLs as single sources of trusted identity. Harmonized regulation on data protection and definition of identity in the case of legal persons will be needed as a preceding step.
- How the right to erasure ("right to be forgotten") will be interpreted. The tamper-proof feature of the DLs conflicts with this right recognised by European regulation on personal data protection.
- The legal framework for the validity of documents stored in the DLs as a proof of possession or existence.
- The legal framework for the validity of financial instruments issued on the DLs.
- The legal framework for smart contracts in general, settlement finality and in international commerce in particular, including real-world enforceability, territoriality and liability.
- The legal framework for the treatment of shared information in DLs from the perspective of cross-border flow of data, and data protection in general. Clarification on whether encrypted data is considered personal data is needed as well as on the right to portability of personal data from one processing place to another.
- Legal framework regarding the use of DLs as a valid ruling register for the IoT.
- Regulatory reporting information standards definition on DLs. Regulators will eventually need to clarify and provide guidance on which regulator has an access to what type of data stored on the ledger and in which situation.
- Conceivably, should we reach a stage where there is a single ledger, clarification would be needed on who should run the permission based DL in the financial sector and who should control the access rights to the network. (e.g. a supra-national organization on a non-profit basis)

While DLT is still at an early stage of development and deployment, its potentially transformative implications raise important questions and considerations for policymakers, regulators and lawmakers as well as for financial services institutions and users. The

potential uses for DLT are numerous and diverse. The regulatory framework needs to be sufficiently calibrated and given the necessary flexibility to take into account the diverse potential applications of DLT that are adaptable to operating across multiple activities and services. Therefore, as previously noted, the adoption of a "one size fits all" regulatory framework for DLT will not be effective or proportionate.

Ultimately, even though DLT poses a number of legal and regulatory questions, we believe that DLT, if appropriately implemented, has the potential to significantly improve the markets and associated regulatory compliance and reporting.

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

Yes.

As noted in our answers to earlier questions (particularly 2.2), the current regulatory and supervisory framework governing outsourcing is too prescriptive and is out of date. It appears to have been prepared on the assumption that firms would outsource activities completely, on an end-to-end basis. However, firms often use technology solutions as "building blocks" to create larger solutions (e.g. the difference between an IaaS and SaaS cloud offering in which the former may be used with a number of applications and is often a means to an end). Some of the building blocks may be retained within the firm and others provided by third parties. The current regulatory and supervisory framework needs to be amended to give firms more flexibility in how they manage the risks associated with using external service providers.

Evidence from other jurisdictions suggests that that the submission requirements for notification/approval are still focused on business processes and the questions posed can prove difficult or impossible to answer for scenarios where what has actually been outsourced is just the technology platform. In response to this we hold that regulators' frameworks need to be overhauled to accommodate the changing technology landscape in financial services, and that they need to be consistent.

Being able to outsource certain tasks which are not part of the core business is an important business model which provide significant benefits including creating a more agile environment capable of delivering innovations more quickly both to the consumer and in the area of technology change.

The use of third party providers is essential for the development of industry wide solutions to industry wide problems (e.g. for the wide adoption of Regtech). Therefore, the issue of third party liability is an important one to appropriately address through the legal framework.

Finally, although it is important to address specific outsourcing regimes, it is also essential to move toward a harmonized approach to outsourcing technology in financial services. Many of these solutions gain efficiency with scale and thus the more barriers that can be removed (one of which is complying with divergent regimes not just in the EU, but in neighbouring countries) the greater the uptake and benefits of the technology will be and thus the greater the benefit which can be passed either directly or indirectly to consumers whether individuals or SMEs.

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

Please see above.

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?

We refer to question 2.1 where we listed the most prominent FinTech use cases.

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?

Banks and FinTech start-ups/non-banking FinTech companies are seeking to test out new technologies, solutions and business models but are sometimes constrained by the existing regulatory framework which does not allow low-risk and low-scale experimentation to take place under less stringent rules. This issue limits competition and may stifle innovation in financial services. Consumers, in turn, are hindered from enjoying certain improved value propositions from their trusted banks.

Examples of 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:

- The regulators' regulatory handbooks, particularly the outsourcing rules, should be amended to give regulated firms more flexibility in how they manage the risks associated with the use of FinTech solutions.

Amendment to the Capital requirement Regulation (CRR):

- Amendment to the CRR: "Article 4 Definitions: (115) "intangible assets" has the same meaning as under the applicable accounting framework and includes goodwill, with the exception of software for the purpose of Article 36 b)".

The banking industry faces digital challenges in competition with emerging technological players that often do not have to face the heavy regulatory burden imposed on the banking sector and are free of prudential regulation altogether. The current regulatory capital framework for credit institutions does not recognize the value of software for capital purposes. The fact that every euro that an EU bank invests in an IT development needs to be backed with one euro of the most expensive category of funding is perceived as a significant disincentive for investments in innovation and a major factor of unfair competition.

FinTech companies are both competitors and partners for the European banking sector. However, when a bank acquires a FinTech company, its main asset- the software, is automatically depreciated given the deductibility that has to be applied to calculate capital levels for banks. If the buyer is a non-bank, the deduction would not be required. This is like assigning a zero value to the search engine of Google if this were bought by a bank. Because of this, banks may be less open to financing these companies.

The regulatory approach to software of the European regulators already acknowledges, to a certain extent, the fact that software has the capacity to generate value, when it comes to the treatment of software for solvency purposes for insurance industry. Under solvency framework for the European insurance industry, intangible assets can be recognized for capital purposes as long as it can be demonstrated that there is a value for the same or similar assets. We believe investments in software should carry the same economic and financial rationale, regardless of the industry. Whilst this may not be sufficient, it sets the basis for the solution to the issue in the banking field. Evidence clearly indicates that software has value even in the case of liquidation of a bank.

Software has become a core asset for the banks business models around the world. However, there is evidence of different regulatory treatment of software in some jurisdictions. In the US

for example, capitalized computer software can be recorded as an "other asset" subject to regular risk rating and not deducted, therefore removing an artificial hurdle to banks investing in digital, while also creating value for the economy as a whole and leading worldwide innovation in the area.

Furthermore, in decisions issues by the European Commission on equivalence of the regulatory regimes of third countries to those applied in the EU capital regimes of third countries that do not require capital deduction for software have not been considered as an element of relevant discrepancy or inconsistency for the European Commission, including for the Basel Committee under its Regulatory Consistency Assessment Programme. This has led us to believe that the non-deductibility of software does not raise an issue.

3.2 What is the most efficient path for FinTech innovation and uptake in the EU? Is active involvement of regulators and/or supervisors desirable to foster competition or collaboration, as appropriate, between different market actors and new entrants? If so, at what level?

The FinTech ecosystem in the EU is robust and growing with the current level of regulatory engagement. As the FinTech ecosystem continues to evolve, regulators should monitor for emerging risks and take action when warranted, as well as ensure that there are no undue constraints on collaboration between institutions.

As noted above, collaboration between banks and startups does not mean that startups are limited in their ability to scale. Policy makers and regulators should consider therefore how to encourage partnerships between large firms and start-ups and between firms of equal size. In addition, because FinTech companies are increasingly in dialogue with regulators and will continue to be with plans for a Regulatory Sandbox, regulators are in a position to identify market opportunities and facilitate partnerships.

> **Recommendation:** regulators should consider working with industry associations to support a referral or referencing tool or service between different firms active in the market who they encounter through any regulatory sandboxes or other activities. This will facilitate the formation of, or strengthen existing, FinTech ecosystems while also not putting regulators in a position where they are directing the market.

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 details.

Each member state has different regulatory bodies with different regulatory appetites and different laws. We encourage regulatory harmonisation, passporting and lower barriers to entry across Europe as well as into Europe from external jurisdictions, implemented through a framework, rather than regulation.

As noted above, collaboration between banks and startups does not mean that startups are limited in their ability to scale. Policy makers and regulators should consider therefore how to encourage partnerships between large firms and start-ups and between firms of equal size. In addition, because FinTech companies are increasingly in dialogue with regulators, regulators are in a position to identify market opportunities and facilitate partnerships.

> **Recommendation:** regulators should consider working with industry associations to support a referral or referencing tool or service between different firms active in the market who they encounter through any regulatory sandboxes or other activities. This will facilitate the formation of or strengthen existing FinTech ecosystems while also not putting regulators in a position where they are directing the market.

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? If yes, 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?

Most of the activities that FinTech undertakes/supports are already regulated via other means – i.e. PD (via current legislation and GDPR), MiFID II, PSD 2, 4 MLD, FSMA/FCA Handbook etc.

If the FinTech in question is a 'company' and is itself undertaking regulated activities, then it will be licensed and will have to comply with any applicable regulatory requirements. If the FinTech company is supporting the activities of a regulated entity, then the regulated entity must ensure it is complying with all relevant regulatory requirements the regulated entity is subject to (in the UK this is covered under SYSC 8 & 13). If the FinTech is developed 'in-house' by regulated entities, then it is already subject to the regulatory requirements that entity has to comply with.

While further detail is required on any proposal from the EC, we note the following general points on the notion of an 'all-encompassing FinTech license':

- We believe that the EC and other relevant regulators must provide a clear and comprehensive regulatory and supervisory framework before the introducing new licensing categories for FinTech activities.
- These licenses should be specific for the activity that the FinTech companies want to perform, to ensure effective supervision of their risks. A closer supervision by the authorities is required to ensure that the services provided by those companies remain under the provisions of that they have been licensed for. Further the type of service providers in transactions should be classified.
- FinTechs should have similar, if not the same, capital/liquidity/consumer requirements for a given activity as a financial institution.
    - A level playing field is needed to ensure fair competition between financial institutions and other FinTech players. Therefore, we support consistent, activities-based standards for FinTechs and emerging business models.
    - Existing FinTech companies often have atypical funding models and complex equity and ownership structures due to their venture capital and private equity investors, and in many cases will also have non-traditional balance sheet compositions that do not fit readily into the existing capital frameworks for banks.
- Discretion should be reserved for activities that are not routine for conventional banks.
- When determining what activities are core banking activities, the question ought to be what activities are necessary for a company to undertake in order for it to be eligible to be licensed as a national bank.
- Related to the issue above, there are financial stability concerns if established tech industry players (Microsoft/Amazon/Apple/Google) and/or merchants are able to seek a limited purpose license in addition to FinTechs (key to this issue is whether non-bank subsidiaries can benefit from the licence). The larger techs/merchants activities would have systemic implications. Any proposal for an EU FinTech licence must have a well-defined scope.
- Issues of consumer protection and financial inclusion must be the subject of consistent, rigorous, and transparent application across FinTech companies and full-service national banks.

There are specific activities that do warrant careful attention by regulators, regardless of who is engaging in the activity – namely payments, lending activities, and data storage – as the risks associated with these activities have far reaching impacts to consumers and the broader financial system (i.e. money laundering, terrorist financing, disparate impact, fraud, identity theft, unauthorized transfers, etc.).

Recommendation: In light of these considerations, we would propose, if the Commission is to explore the notion of a FinTech licence as suggested in its CMU mid-term review, that it consults publicly on its design.

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

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? If so, please explain in which areas and how should the Commission intervene.

As above, we support consistent, activities based standards for FinTech and emerging business models.

Please see below comments on the Regulatory Sandbox in 3.8. We note that in order to achieve maximum effectiveness, any Regulatory Sandbox should have the mechanisms for sharing of regulatory learnings across different regulators, EU jurisdictions as well as with other national regulators. We thus encourage the EU to pursue official agreements with other national Sandboxes in operation around the world.

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? To what extent regulations on data localisation or restrictions on data movement constitute an obstacle to cross-border financial transactions?

Banks have local law banking secrecy/client confidentiality obligations in addition to general data protection requirements to consider when flowing data both within and out of the EU.

Data localisation

Data flows are an integral part of companies' daily trade and operations. Their ability to transfer data throughout the world is vital including for banks, no matter their size or the geographic area in which they operate. Data localization laws complicate cross-border business strategies, limit choice of service provider and hinder the ability to provide products and services to global customers.

Prescriptive regulations on data localisation are at odds with trends in technology. The latter, unlimited by geographic boundaries, can manage storage and access to data, located globally.

We observe that several EU countries have introduced, at national level, additional limitations and barriers which prevent data circulation and intra-group synergies at EU and international level. These have an impact on risk management, centralised/shared infrastructure strategies, and the ability to provide products and services to global customers.

Banks need to be able to transfer data across borders effectively so as to respond to customers' needs: delivering goods and services, processing payments or providing customer support. To achieve cross-border data flows, there must be no direct or indirect restrictions on data localisation. Limiting data flows without objective and justified reasons undermines the ability of companies to define their business models; it will be detrimental to competitiveness and growth of EU companies; and, endanger the functioning of critical infrastructure.

We would argue that whilst Member States' interests in national security and law enforcement are fully legitimate in most cases (not least those linked to non-personal data), there is no valid

justification for data localisation. In practice, these interests are too often used to justify, largely unrelated, measures. We agree with the Commission's statement that localisation restrictions rarely advance the public policy objectives they are intended to achieve.

We support any EU initiative that could remove restrictions to the free flow of data which at the same time acknowledges the right that businesses have to choose where they store their own data. Companies' decisions on data localisation may be part of a specific business model and companies must be allowed to request or provide data localisation. This is a choice made by both providers and recipients of the service, which is quite different from a legislative obligation to do so.

Cloud

As previously noted, one of the hindrances to a consistent European Union (EU) and Global regulatory framework for Cloud Computing in Financial Services is related to regulation and domestic laws which establish barriers to the geographic location of the physical Cloud Computing infrastructure. Frictions to leveraging the benefits of Cloud Computing in Financial Services arise when data regimes restrict cross-border data flows, both within the EU and globally.

Data stored in a Cloud Computing environment can be fragmented geographically and its support functions (such as processing, hosting, backup, support and management), divided among suppliers (often across national boundaries) to enhance their data security, disaster recovery and resilience. In this regard, this progress in technology towards a 'distributed' network infrastructure challenges traditional data and outsourcing concepts such as the physical data localisation and auditing of physical premises.

According to the financial rules on outsourcing for many EU countries, financial institutions must notify the supervisor and obtain their approval to launch cloud projects. This notification and approval has to be done on a case by case basis. It implies an indirect constraint to the free flow of data and, thus, to a faster innovation and a more agile cloud adoption. There is a need to harmonize EU financial supervisors' criteria when approving cloud projects. The EBA's guidelines on cloud currently out for consultation go some way toward helping institutions navigate this inconsistency, but a more thorough review of outsourcing rules would create efficiencies and encourage the use of cloud computing in financial services.

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

Yes they are appropriate. We would reiterate and elaborate the following points that the Commission should consider in its regulatory approach to FinTech activities:

- A one-size-fits-all regulatory approach is not conducive to technological innovation. Any regulatory framework should be flexible, graduated and principles-based, with oversight tied to scale and the risks presented.
- Associated with this is the need to focus on frameworks and not specific technologies or companies.
- New rules or guidance should take into account banks' existing authorities to develop, test and launch innovative products and services. It is also important that regulators do not implicitly limit the ability to experiment – there can be no reward without some risk and thus it must be acceptable for some new initiatives not to work out.
- Specific activities warrant careful attention by regulators, regardless of who is engaging in the activity – namely payments, lending activities, and data storage. The risks associated with these activities have far reaching impacts to consumers and the broader financial system (i.e. money laundering, terrorist financing, disparate impact, fraud, identity theft, unauthorized transfers, etc.).

Regulators and supervisors must be prepared to develop new expertise and engage both banks and non-banks in order to understand the fast moving changes happening in the market. The industry stands ready to assist regulators in knowledge sharing and we look forward to developing a mode of interaction that ensures innovation comes to the market quickly, efficiently and above all, safely.

Stringent prudential, security, investor and consumer protection regulation are an inherent part of the regulatory framework in which banks have to operate and which has been reinforced in recent years. New entrants are less burdened by regulatory requirements and they tend to choose the optimum legal structure to avoid the heavy regulatory burden of the financial sector. Similarly, they are not subject to the same levels of scrutiny from supervisors and authorities. The implications of this for policy objectives concerning consumer/investor protection, fraud and financial crime, and financial stability must therefore be considered.

From a supplier's perspective, the concern is that a loss of trust by consumers in one area of the industry, whether that be a FinTech start-up or a large incumbent, hurts the sector as a whole. With equal rights must come equal responsibilities. Cybersecurity is a good example of this principle. A failure by any single market participant hurts the reputation and damages trust in the industry as a whole. Policy makers should consider the importance of ensuring that a regulatory standard is applied and supervised across all market participants.

The Digital Single Market is an opportunity for all operators willing to embrace the digital transformation: authorities, banks, FinTech start-ups, corporates and consumers. It is important to promote innovation and avoid unintended disincentives: regulation can often also be observed as a disincentive to experimentation. Undertaking regulated activities in various Member States usually requires explicit permission from the regulator and approval of the way in which the firm in question goes about its business. A risk-averse regulator may not be willing to grant permission to unfamiliar or unproven business models. Unregulated entities may, however, find it easier to undertake new business without having to comply directly with the regulator's tests. Similarly, digital services can easily cross borders, and varying risk appetite among regulators and overseers may hamper the cross-border provision of services and unintendedly lead to market distortion.

Finding a proper balance, and future-proofing it, will be one of the main (and on-going) challenges for policymakers, regulators and supervisors for the years ahead: how to encourage the development of financial technology and to bring dynamism and competition into the financial sector both for incumbents and new entrants without leaving the financial sector open to new risks or significant failures and thereby endangering financial stability, with possible loss of public confidence, or creating an uneven regulatory framework. Customers and investors' trust will be gained if they are confident that the same level of protection is available no matter which entity – banks or non-banks alike – is providing the financial services.

Technology (and digital platforms) neutrality and cooperation are also important concepts in this respect, as otherwise an uneven playing field will be created that will see a number of businesses including banks face competitive disadvantages from certain competitors that control digital platforms on which banks and many other businesses often depend for offering their digital services. We thus promote the following considerations:

1. Allow for competition to unfold: a number of adjustments to existing legislation / regulatory frameworks and right-sizing of regulatory requirements need urgent attention for competition and if a Digital Single Market for financial services to take off, and must be addressed in the short term.

2. Put Digital first: a thorough fitness check by the EU of the existing complex regulatory framework is necessary to ensure it is fit for purpose to support banking in the digital age. To be clear we see no need to create new regulation for the digital era but consider it important to make a thorough and comprehensive review of existing legislation to ensure the current framework is up to date, future-proof and does not impede innovation and

competitiveness in the Digital Single Market for financial services. Furthermore, regulation must not unduly constrain banks or FinTech start-ups from providing an effective response to the challenges posed by digitalisation.

3. Have a clear policy for how to engage with technology while maintaining neutrality: There are a number of technologies under development or coming to market which have a direct impact on regulators and supervisors be that RegTech solutions or potential new market infrastructures, for instance some DLT solutions. While recognising the neutrality implications of engaging with any specific technology or market solution, we do not want to see regulators become a bottleneck to innovations which could help the market. Therefore, we encourage regulators to immediately begin gathering an understanding of these technologies and working towards the development of a clear policy that will allow for progress while providing clarity to the market in such a way that competition is not damaged.

3.8 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? Would there be merits in pooling expertise in the ESAs?

A FinTech incubator, coordinated by the European Supervisory Authorities and promoted by the European Commission, could be an excellent opportunity to collect new ideas, identify new innovative services, monitor trends and address innovation especially in the perspective of potential regulatory adjustments and integrations.

Regulatory Sandbox

Authorisation can be a lengthy and expensive process which deters FinTech start-ups from working within regulated activity and hinders innovation. The authorities must provide FinTech start-ups and banks which innovate with leaner and faster authorisation processes. A market friendly approach which balances the length of time to market and customer protection would be a supportive approach to authorisation.

We support the development of an EU framework for experimentation, especially for new entrants. We understand such a Sandbox to be a safe space in which both incumbents and new players can test innovative products, services or business models in real world environments with guidance from the regulator and with the potential to do so without full compliance with applicable regulations. This environment will allow companies to develop new products and services within a specific regulatory framework, avoiding post-development inefficiencies and sanctions while also giving the regulatory certainty of consumer protection.

In the UK, the FCA has set up a Regulatory Sandbox that allows businesses to test innovative products, services, business models and delivery mechanisms in a live environment. Although there are areas where we think this could be improved, for example the greater participation and sharing of regulatory learnings with other regulators, the general approach is one we support.

Such a regulatory framework for experimentation will allow the regulators to assess new products at an earlier phase and potentially amend legislation rapidly when beneficial to consumers. This approach enables a more forward-looking assessment by financial supervisors and could ultimately lead to new regulatory and supervisory approaches. Ultimately, regulators and FinTechs need to work together to protect customers and build trust.

If structured and supervised correctly, regulatory sandboxes have the potential to facilitate robust dialogue between banks, non-bank FinTechs and regulators on policy barriers to partnerships or deploying innovative services and technologies. An example of a solution that could emerge from such dialogue is regulators being involved in the testing of multi-bank DLT

projects where the regulator could observe its "regulator node". We encourage the Commission to consider this and note that it could provide useful learnings for the regulators.

It is important that authorities do not stifle innovation in established financial institutions. Therefore we believe participation should remain voluntary for established financial institutions, as we already have robust controls and risk management processes in place. Furthermore, we also understand that an EU-wide approach would be challenging because the supervision which remains a key aspect of the regulatory sandbox concept, generally remains at national level. We believe that the development of an EU framework for regulatory sandboxes will help avoid fragmentation of the market and could facilitate intra-EU cross-border expansion of successful FinTech projects.

We encourage the EC and the ESAs to look into a coordinated EU approach on sandboxes, based on the ongoing harmonisation of national frameworks, the adoption of guidelines or principles, and the identification of best practices, as we believe a combination of both national and European framework would work best. Sandboxes must be open to all innovators, with a minimum set of requirements established for all players to ensure a level playing field without stifling new players. However, once a product leaves the sandbox, there must be a level playing field ensured for all providers of digital financial services by applying the same rules required of financial institutions to new entrants.

Finally, in order to achieve the goal of being a "FinTech Hub" any sandbox should have as a guiding principle an open and cross jurisdictional approach, including beyond the EU. Forming connections and allowing for the flow of regulatory learning on technology to jurisdictions outside of the EU will be essential in making the EU a hub for the development of FinTech solutions. A successful hub for technology development must be global in its approach. We thus encourage any EU Sandbox to pursue official agreements with other national Sandboxes in operation around the world.

> **Recommendation:** Given the potential policy implications, within EU and internationally, we suggest that the design of any EU-level sandbox is consulted upon first. The industry has wide experience dealing with a number of different regulatory Sandboxes and would welcome the chance to provide insight on the pros and cons of different models.

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? If yes, please specify how these programs should be organised?

In general we are supportive of collaboration between industry and policymakers. We would welcome an "Innovation Academy" set up by the European Commission in association with other regulators/policymakers from non EU jurisdictions, coordinated by the ESAs and supported by financial (and non-financial) associations (both in the EU and non EU jurisdictions), which could help to train subject matter experts with common background, able to spread the FinTech culture of innovation and to promote the development of innovative solutions.

We recommend that European Commission look to successful model already in practice such as the Bank of England FinTech Accelerator with their new FinTech Community. We also welcome improved dialogue on FinTech discussions within existing fora such as the European Data Protection Board (EDPB), ENISA as well as the European Supervisory Authorities.

3.10 Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS? Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate

cross-border? If so, who should run the sandbox and what should be its main objective?

While sandboxes are incredibly useful tools and foster innovation, we need to ensure that this innovation is for customer benefit and without agenda.

We believe national approaches within the EU 27 would not be helpful in a multinational and global financial industry. The main risk of a national approach might be to create a fragmentation with different approaches among the EU Member States, with the final result that neither financial institutions nor consumers can benefit from these initiatives.

We welcome a global approach to sandboxes– e.g. harmonised criteria for entry, simple and transparent authorisation process – to avoid un-level playing field and to facilitate successful innovations are implemented across Europe and non-EU jurisdictions with minimum delay.

The initial principles for consideration are as follows:

- Clear and simple conditions for experimentations;
- Security, consumer protection and competition rules safeguards;
- Access for all suppliers both regulated businesses and non-regulated businesses;
- Participation should be voluntary for established financial institutions, as we already have robust controls and risk management processes in place;
- Education with guidance on the interpretation of the legislation in relation to the testing activities;
- No enforcement action/infringement procedures during the testing phase;
- Exit and transition strategy should be clearly defined in the event that the new solution has to be discontinued, or can proceed to be deployed on a broader scale;
- Ex-post assessment.

3.11 What other measures could the Commission consider to support innovative firms or their supervisors that are not mentioned above? If yes, please specify which measures and why.

Key issues FinTech companies face include funding, access to organisations, leveraging bank schemes (eg partnerships, accelerators, mentoring, support).

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

3.12 Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision? Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities?

We strongly believe that the Commission's approach should continue to look at outcomes, be technology agnostic, and, if needed, regulate based on the products and services that are offered. It is undesirable that supervision or regulatory requirements are based on generic labelling of institutions as 'FinTech'. We believe that – in line with the objectives of the European Commission and the ESFS – standards are of central important to systemic risk management and subsequently end-user protection. Standards can work as an enabler to unlock opportunities for new entrants and for enterprise-wide regulatory risk management by bringing together the regulatory framework on an ongoing basis.

However, we do not believe that the European System of Financial Supervision (ESFS) needs to play a more proactive role in the development of standards. Various standards for

many types of transactions and services have been defined in the banking sector over the years. Furthermore, the complexity of the standards makes the process of definition and sharing among the players complex as it is necessary to take the operating and technological needs of all of them into account. Instead we believe that there are opportunities to promote global standards in a way that would support the objectives of the European Commission.

The European Commission and the ESFS could look at promoting the adoption of global standards before considering jurisdiction based standards. We see this benefiting the objectives of the European Commission and the FinTech Industry because FinTech is global in nature and therefore the use of standards to support competition, manage risk and promote interoperability should be considered from a global perspective. By its very nature, FinTech often includes products and services that are not jurisdiction-specific – such as data processing, cross-border payments, settlement reconciliation. It would therefore almost always be counterproductive to seek to move towards anything other than global standards.

We note that the current level of data standardisation and interoperability is an obstacle to taking full advantage of outsourcing opportunities. Trade Associations are a possible route for helping to formulate solutions.

3.13 In which areas could EU or global level standards facilitate the efficiency and interoperability of FinTech solutions? What would be the most effective and competition-friendly approach to develop these standards?

The consultation paper correctly identifies that standards create common understanding and promote interoperability, allowing new products and services to connect and interact with existing and developing financial infrastructure in an efficient and secure manner. In the context of FinTech, the objectives of efficiency and interoperability can only be enabled by standards if they are developed at a global level, are outcomes based, technology agnostic, transparent, and inclusive. We believe that existing mechanisms (e.g. the ISO governance and procedures for developing and maintaining new and existing standards) or work within international fora (e.g. IOSCO, FSB) and European and international trade associations provide for this. As global regulatory bodies (FSB/IOSCO/Basel) continue to monitor this space, the Commission should continue to engage to help coordinate FinTech-focused policies.

We also note that the use of global standards could enable other pieces of work that could suit the objectives of the European Commission. Not only does the use of global standards remove the need (and cost) of developing new standards, it also minimises difficulty to those already familiar with global (ISO) standards. For example, we note that the consultation paper looks at the possibility of a role for the European Commission in developing sandboxes. We believe that standards would play an important role in providing interoperability of sandboxes and/or their participants. Standardising onboarding processes, semantics, and financial messaging standards are examples that would benefit the use of sandboxes across the European Union.

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? What other specific measures should be taken at EU level?

This does not appear to be an appropriate role for EU Institutions. The development of libraries of open source models and solutions is so rapid that acceptance by institutions of spreading of standards could slow down the exchange of information and the free choice of the best standards with respect to the needs of each party.

Technology service providers and other owners of intellectual property can choose whether to make their solutions available on an open source basis.

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

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.

FinTech, considered generally, can improve safety and soundness by reducing errors and making the firm more efficient. Data analytics / Big Data, for example, can be used to provide a more granular and holistic view of the firms risk exposure.

Collaborating with other FinTech companies can also bring efficiencies and improved services/products, by connecting external ideas with incumbent knowledge, data, space and other resources to co-create solutions

Where incumbents are able to on-board technology solutions (whether through M&A or commercial relationships) which allow them to remedy issues created by complex legacy systems and manual processes, this is likely to be a big driver of efficiency. However, as per above, the process is not always easy for regulatory compliance reasons.

At the same time, FinTech solutions can potentially build legacy systems on top of legacy systems. It is important to note that new technology is not always the answer.

4.1 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?

Free flow of data will likely be an enabler to the success of a Digital Single Market and improve competition in financial services. It should enable data to be harnessed for improved customer experience and to offer new services within the industry. See question 3.6 above.

Service users and the use of their data should continue to be protected by EU privacy laws (e.g. the forthcoming GDPR and e-Privacy). This should ensure transparency and control is provided to service users. Current and forthcoming data protection legislation provides consumers with adequate protections and greater transparency into how their data is used and ability to consent and opt-out, and also ensures that service providers do not process data for purposes that go beyond the purposes for which the data were collected. This provides appropriate protection, limiting the need for a system of compensation in return for data use.

Where the use of data goes beyond the service providers direct relationship, the need to ensure service user have a transparent choice and control over the use of their data is much greater. Many service users may not yet fully comprehend the value of their data and the consequences of any further processing by service provides. Service providers should be held accountable for ensuing service user education to ensure fair outcomes. It may be important to articulate benefits of analytics to clients/customers for which see chapter 1 above.

4.2 To what extent could DLT solutions provide a reliable tool for financial information storing and sharing? Are there alternative technological solutions?

The financial services industry already has a range of tried and tested solutions for storing and sharing financial information. New technology and processes are constantly reviewed to assess whether they can provide efficiencies or improve services. DLT is no exception and the financial industry has been investigating the potential merits of this technology for several years. It is not a panacea, but there are some specific use cases where DLT might offer reliable solutions. So far many of the most useful solutions have appeared in the post-trade environment, however, over time we expect to see other solutions making use of DLT technology. For example, there are many financial processes and services that could benefit from the immutable nature of DLT storage. Contract information, property rights, and in general “digital fingerprints” of any kind of agreement (even when signed off the ledger) are some of the types of information that could potentially be stored in a Distributed Ledger.

We also see DLT as complementary to APIs. DLT is generally better for pushing or broadcasting data, APIs are good for pulling data. DLT by itself is generally not really suited to be an information store, but is good for data synchronisation between multiple organisations. Generally speaking, distributed ledgers have a lot of embedded attractions (e.g. cryptographic integrity, smart contracts) that are not always present in conventional tech. In addition, distributed ledgers are agnostic - i.e. one can use a distributed ledger to persist identity of individuals real or corporate (really a collection of facts/contracts). Individuals and things can be ‘defined’ using these facts and the distributed ledger is ultimately just a way of addressing and indexing these arbitrary facts.

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

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

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

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

It should be noted that for certain DLT uses cases, digital identity frameworks, considered at the individual / end-investor level, will not be an obstacle – e.g. for DLT applications with institutional participants as nodes, which will likely utilize a more typical account structure and permissioning approach to manage client "identity."

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

Data held within DLT is very likely to be encrypted. However, with continuous increases in computing power and technology advances, we assume that any encryption applied today will be compromised in the future, maybe in 3 years, maybe 20 years.

Therefore, we would treat DLT the same as any other technology in regard to personal data protection. Personal data should only be shared with parties that have explicit permission to see the data, regardless of encryption.

For DLT this leads to two scenarios that can be applied to data sharing:

- The DLT does not hold personal data, but may hold pointers to where the data is held.
- The DLT supports scenarios where the data elements are only shared with a specified subset of network participants, not all participants.

There are various forms of DLT solutions, including solutions where the data is accessible only to users who have been given appropriate access. The existing legal and regulatory framework provides sufficient protection. To introduce regulatory requirements specifically for DTL solutions would be contrary to the Commission's stated objective of being technology neutral.

Restrictions on transfer of data across national borders potentially creates a challenge for use of DLT solutions. However, the same applies to other technology solutions, e.g. cloud computing solutions.

4.5 How can information systems and technology-based solutions improve the risk profiling of SMEs (including start-up and scale-up companies) and other users?

Start-up and scale-up companies are very difficult to risk profile. Each is unique and requires extensive work to understand the business, hence it is also very difficult to make comparisons.

Big Data technologies may allow more information to be acquired from SMEs, reducing the credit risk and financial risk. IOT could also support acquisition of data on the assets of SMEs and improve risk profiling. In particular, in capital markets, the availability of information on companies, especially medium and small sized companies, is an important factor for potential investors on investment opportunities, to the advantage of the target firms and the economy as a whole.

Overall, any innovative use of customer data for lending purposes should be consistent with responsible lending principles.

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?

Data protection and customer confidentiality requirements restrict Banks and other financial services firms from sharing information on their customers with third parties, whether SMEs or other categories of customers.

In the UK, there has been a move to require large banks to share credit data on their SME customers with competitors via credit reference agencies. The large banks are seen as having a competitive advantage over alternative finance providers and smaller lenders by having access to large pools of information on their SME customers. The idea is that sharing specified information with smaller lenders and alternative finance providers would make it easier for these lenders to check the credit worthiness of potential borrowers which

in turn would lead to increased competition among the lenders and open more opportunities for SMEs to access finance.

One risk to SMEs in this context is that this access to information may not help a key part of the SME market, i.e. start-ups. Start-ups would not necessarily have sufficient credit history which could be shared in the way envisaged by the credit sharing arrangements. The concern is that for a borrower without a track record, competition amongst lenders may not have the desired impact of lending on more favourable/competitive rates.

Another risk that has been identified is that the information shared gives only part of the picture of an SME's credit risk, and that could lead to less favourable lending rates than would otherwise have been available had the lender had a more complete picture of the performance of the business.

Data protection is a key risk which underlies the sharing of information, particularly if it is proposed that information would be shared cross-border.

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?

No additional requirements are needed. Financial institutions are heavily investing in their IT systems including cyber-security measures as well as their incident response and resiliency capabilities. Technology innovations – including Internet of Things, artificial intelligence and cloud – open the door for increasingly complex cyber threats and solutions.

Cyber-security is particularly relevant when FinTechs collaborate with financial institutions, as end-to-end security across the whole financial services chain must be ensured. Therefore, any solution offered by FinTech companiess based in new technologies should be built with privacy and security considerations by design and appropriate testing should be done before releases into market. This applies also to large software companies where there seem to be relative lack of control and supervision from a security standpoint.

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

Regarding any regulatory approach to cybersecurity, we would stress that effective cyber defence requires a global perspective. These efforts require constant collaboration and strong partnerships to counter innovative threat actors and evolving risks. As such, financial firms must collaborate with government partners around the world, other financial industry partners, as well as vendors and clients to effectively address cyber threats.

We strongly support regulatory harmonization by global supervisors around risk-based approaches to cybersecurity risk management. The G7 "Fundamental Elements of Cybersecurity for the Financial Sector" provide a starting point for all cybersecurity regulation; we consider the NIST framework to be an example of an instantiation of the principles defined in the G7 "Elements".

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?

Cybersecurity:

As recent events have demonstrated, cyber security is not an issue specific to any one industry. Although the financial services sector has made significant progress on this front as demonstrated by its relative resilience to the recent global ransomware attack known as Wannacry, the industry remains alive to the need to do more and improve security. Firms often collaborate with other members of the financial industry beyond interaction with governments and regulators. The belief that cybersecurity is not a competitive issue has allowed the industry to work together to improve the cyber defences of the sector as a whole. Information sharing and coordinated analytic work have been the hallmarks of sector collaboration. We support the rules as drafted in the EU Network and Information Security Directive and calls on national governments to ensure consistent implementation of the Directive.

Having said this, the EU could play a role in:

- **Harmonising/streamlining the format and procedures for security (IT) incident reporting.** Such progress is vital to avoid overlap and redundancy in reporting to multiple competent authorities (NIS Directive, PSD2, Data protection regulation, Single Supervisory Mechanism SSM) which in turn will not only allow the industry to react more quickly and effectively to attacks, but also to better anticipate threats and move to prevent incidents, which must be the ultimate goal.
- **Establishing a legal framework for data sharing for resilience and risk mitigation purposes.** Such a framework should allow the sharing of sensitive information related to fraud & cyber-attacks at national and cross-border level.

We must continue to improve collaboration between industry and regulators, and also collaboration among regulators, to make meaningful progress in effectively meeting the evolving threat posed by cyber attacks. The public sector needs to work proactively with the private sector, across borders, to share information about attacks, exchange best practices and continually improve security systems to deter cyber criminals. As previously mentioned, cybersecurity must be considered a global issue, therefore cooperation among jurisdictions is vital.

All players, including FinTech companies, should be able to share on a cross-border level cyber threat intelligence and cyber incident information through reliable and safe tools and mechanisms in order to increase cyber resilience.

The different interpretation of privacy guarantees in the various European countries creates difficulties in managing the necessary exchange of information in order to share cyber threats. The LEA could improve cross border collaboration in the exchange of information that is useful in preventing and resolving cyber attacks and cyber fraud.

There are a number of bodies active in the UK and the EU through which cyber threat intelligence is shared including ones where closer information-sharing occurs. However, there are challenges in certain jurisdictions in relation to data privacy in respect to what is personally identifiable information (e.g. IP address) which not only makes information-sharing difficult, but also makes monitoring to prevent activity problematic.

Recommendation: The recently introduced exclusion for prevention of fraud within GDPR should be extended to cybersecurity prevention and monitoring.

It is also the case that new requirements on GDPR inhibit or provide obstacle to appropriate monitoring of insider threat and collaboration with law enforcement, government agencies and wider industry.

Recommendation: A legal construct akin to the Joint Money Laundering Taskforce (JMLIT) is needed to provide full legal cover to allow greater cyber security information sharing at national and EU level. The focus should not only be on improving cyber

defence (predict, prevent and protect), but also on making it risky to be a cyber-criminal (prosecute).

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)?

We consider that penetration tests by third parties introduce operational and data risks. Therefore we support firms conducting their own penetration tests in partnership with the regulatory community, based on the framework GFMA has developed.

Many firms operate robust, intelligence-led and threat-centric penetration testing programmes. However, it must be acknowledged that they lack the necessary controls on large established software companies who may introduce vulnerabilities globally.

We are supportive of EU level penetration testing if done correctly, i.e. along GFMA guidelines, to the extent that it would further regional coordination. One current hurdle is the variation of regulatory expectations across multiple jurisdictions. We are also supportive of a safe and scalable approach to regulatory penetration testing and red teaming across the entire EU wherein single test results satisfy multiple supervisors' requirement (hence limiting the operationally risky execution of penetration tests or red team assessments).

There may be an opportunity for harmonisation of the testing of financial institutions and other FinTech companies through alignment to exiting frameworks. Sector specific cyber wargaming such as "Waking Shark" may enable improved understanding for regulators of the capabilities of market participants and also sector level improvements. However, the focus mist remain on firms conducting their own testing in partnership with regulators and authorities.

4.10 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? Are there any regulatory requirements impeding them?

It is noted that the GDPR creates a new right of 'data portability' with effect from May 2018, which is intended to facilitate switching between different service providers, and will foster the development of new services in the context of the digital single market strategy and generate competition. 'Data controllers' will have to develop download tools and Application Programming Interfaces. Guidelines issued by the Article 29 Working Party (EU data privacy regulators) encourage industry stakeholders and trade associations work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability.

Technologies which enable the secure access / transfer of data and robust mechanisms to ensure authenticity of access requests from other service provides which demonstrate authority from the service users.