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

INVESTMENT AND COMPANY REPORTING
Economic Analysis and Evaluation

Reply form for the Consultation Document "FinTech: A more competitive and innovative European Financial sector"

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

INVESTMENT AND COMPANY REPORTING
Economic Analysis and Evaluation

Date: 15 June 2016

Responding to this paper

You are invited to reply by 15 June 2017 at the latest to the online questionnaire available on the following webpage:

https://ec.europa.eu/info/finance-consultations-2017-fintech_en

Please note that in order to ensure a fair and transparent consultation process only responses received through the online questionnaire will be taken into account and included in the report summarising the responses.

This consultation follows the normal rules of the European Commission for public consultations. Responses will be published unless respondents indicate otherwise in the online questionnaire.

Responses authorised for publication will be published on the following webpage:

https://ec.europa.eu/info/finance-consultations-2017-fintech_en#contributions

Executive Summary

The Association for Financial Markets in Europe (AFME) welcomes the opportunity to share our views on the Consultation Paper issued by the European Commission on Fintech published on 23 March 2017 with a deadline for a response by 15 June 2017.

Please do not hesitate to contact Emmanuel Le Marois on 44 0203 828 2674, email Emmanuel.LeMarois@afme.eu, or David Ostojitsch on 44 203 828 2761, email David.Ostojitsch@afme.eu, should you wish to discuss any of the points.

AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia. AFME is listed on the EU Register of Interest Representatives, registration number 65110063986-76.

It is important to define FinTech in order that AFME's response to this consultation can be correctly understood. FinTech encompasses a broad number of actors and participants. Some are small innovative companies, others are large incumbent financial firms looking to acquire or work with startups to drive innovation, others are even existing technology companies providing new financially focused tools. These can all legitimately be described as FinTech.

AFME's preferred definition of FinTech therefore is: "Innovative computer programs and other technology used to support or enable banking and financial services".

- AFME believes that **FinTech can deliver a more competitive and innovative financial sector;**
- AFME **advocates regulation of the activity taking place not the technology that delivers it**;
- The EU FinTech ecosystem is strong and growing with the current level of regulatory engagement. As the FinTech ecosystem evolves, regulators should **monitor for emerging risks and act when warranted, while ensuring there are no constraints on collaboration** within the ecosystem. Engagement beyond this may have unintended consequences;
- **A strong focus on standards and interoperability** will speed adoption and drive collaboration;
- **Successful FinTech adoption should reduce costs for existing financial institutions**, improving their ROE and making more funds available for the real economy to empower growth;

- **Any framework should take into account banks' existing authorities to develop, test and launch innovative products and services**;
- **Any new regulatory framework should be flexible, graduated and principles-based**, and oversight should be tied to scale and the risks presented;
- **Certain activities warrant careful attention by regulators**, regardless of who is engaging in them, **as the risks associated with these activities have far reaching impacts to consumers and the broader financial system**;
- The **EU can help accelerate the achievement of these goals by supporting regulatory harmonisation, the adoption of universal standards, increasing interoperability and promoting risk capita**l;
- **The EU can provide specific support** via:

    i) **Promoting standards** around data and cyber security to prevent a fragmented digital EU landscape;
    ii) **Driving go-to market efficiency**;
    iii) **Harmonisation of practices** for outsourcing;
    iv) **Adapting the regulatory framework**;
    v) **Increasing global alignment** around standards;
    vi) **Facilitating knowledge transfer**;
    vii) **Increasing training**.

- AFME considers it important to **develop a common EU framework for crowd funding** to improve access to risk capital and protect retail and semi-professional investors. Regulation should be proportional to the risks being taken;
- AFME members see the **long-term benefits that will arise from the adoption of Distributed Ledger Technologies (DLT**) such as:

    i) **More efficient post-trade processes**;
    ii) **Enhanced reporting and supervisory functions**;
    iii) **Greater availability and security**;
    iv) **Reduced counterparty risk** and enhanced collateral management.

- However, AFME members feel **that significant challenges remain** before wide scale adoption is achieved due to legal, regulatory, technical and operational factors.

1. FOSTERING ACCESS TO FINANCIAL SERVICES FOR CONSUMERS AND BUSINESS

Question 1.1:

- *What type of FinTech applications do you use, how often and why?*

AFME supports the growing use of FinTech within the wholesale markets, noting that Fintech provides opportunities for more efficient customer servicing at lower costs and we view that FinTechs can be classified in (but not limited to) the following areas: crowdfunding, cloud computing, outsourcing, robotics and distributed ledger technologies (DLT).

Within each of these areas, FinTech provides users the ability to:

i) **enhance business models**;
ii) **rationalise costs**;
iii) **enhance customer servicing**;

AFME members support a collaborative approach to working with FinTech within the wider eco-system and we note that the success of this collaboration is ultimately dependent on certain factors, which determine the incentive to innovate (e.g. risk appetite, the amount of investment capital available, scalability, skills, competition and regulatory approach).

- *In which area of financial services would you like to see more FinTech solutions and why?*

AFME would like to see more FinTech solutions in areas that could help the industry:

i) **achieve regulatory compliance** (e.g. RegTech);
ii) **become more agile** with their business (e.g. resilient to change);
iii) **have increased transparency and control** over their data and processes (e.g. process and application integration);
iv) **operate more securely** (e.g. cyber).

Innovation will depend on the ability for market participants to comply with regulatory requirements and the amount of capital available for innovation. AFME believes that clarity on regulatory requirements and facilitating venture capital will benefit the development of FinTech in Europe.

This could be accelerated by means of harmonising regulation, adopting universal standards, increasing interoperability between solutions and promoting risk capital in Europe. On the latter, a study by the Wall Street Journal demonstrates that only 4 out of the 17 global "Fintech unicorns" are in Europe (see table below). AFME believes that this is due to a EU fragmented internal market, with different regulations, taxes and standards contributing to a shortage of risk capital.

Table:

Financial Services unicorns (companies with last estimated valuation larger than $1bn)		
Company Name	Country	Estimated valuation (bn$)
Lufax	China	18.5
Stripe	US	9.2
Whong An Online	China (HK)	8
One97 Communications	India	4.8
SoFi (Social Finance)	US	1.4
Credit Karma	US	3.5
Mozido	US	2.4
Ayden	Netherlands	2.3
Avant	US	2
Prosper Marketplace	US	1.9
Lakala.com	China	1.6
Klarna	Sweden	1.4
Robinhood	US	1.3
TransferWise	UK	1.1
China Rapid Finance	China	1
Funding Circle	UK	1
Kabbage	US	1

Sources: Wall Street Journal

1.1. Artificial intelligence and big data analytics for automated financial advice and execution

Question 1.2.

- *Is there evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services (investment services, insurance, etc.) and at what pace? Are these services better adapted to user needs? Please explain.*

Yes. AFME believes that automated financial advice (robotics) is a key innovation in financial services as they facilitate a 24/7 operation faster at lower costs. For

example, robotics could be of increased value in areas where data gathering/processing can be time intensive, where delivery of customer service could be inconsistent and where specialist advice is provided in niche areas (e.g. wealth management, portfolio management and tax advice).

Robotics are also expected to provide a more automated audit chain due to the electronic nature of their operation and are expected to be configured to be compliant by design and embed the appropriate control mechanisms, which could also lend itself to internal as well as external processes.

However, at this time widespread use and adoption of robotics remains a challenge. We believe that this is mainly due to development and implementation costs which may currently outweigh the benefits. Automation and robotics are still a burgeoning industry where, i) process automation, ii) natural language generation, iii) cognitive learning and iv) artificial intelligence, are profoundly different solutions which could be adapted to different needs.

Robotics as seen by Cognizant consulting[1] can be divided in three clusters: (i) Systems that do: Robotic Process Automation, Data collection/Data Preparation, Speech-to-Text Conversion (ii) Systems that think: Autonomic Automation, IT Process Automation, Smart API's, Natural Language Processing (iii) Systems that learn: Machine Learning, Sentiment Analysis, Cognitive computing, Artificial Intelligence, Deep Learning, IoT & Smart Devices

Question 1.3.

- *Is enhanced oversight of the use of artificial intelligence (and its underpinning algorithmic infrastructure) required?*

No. AFME's view is that regulatory oversight of the use of artificial intelligence is not required, however we would encourage the adoption of best practices and standards for the design and implementation of the technology.

Artificial Intelligence (AI) is a nascent and burgeoning technology which requires further development. We think that further investments are required to overcome the current challenges of data availability such as converting unstructured data into structured data, extracting data from legacy systems, integrating with the overall IT architecture, which would extend the benefits of AI. Furthermore, we believe that non-harmonised regulation could pose additional barriers to innovation.

AFME believes that AI, and in a wider sense robotics, offers the following benefits:

[1] Cognizant Consulting, White papers, "Bots at the Gate – Intelligent Automation: Where we stand – and where we're going", Matthew Smith, 14th September 2016

i) **Efficiency gains**: 24/7 availability, faster, fully auditable processes at lower costs;
ii) **Client servicing**: Enhanced customer servicing, broader, more bespoke and more consistent approach.

Therefore, AFME's view is that the regulatory approach should be technology agnostic and focus on the usage and outcomes. We recognise as the technology develops, there may be new risks to manage, which should be closely monitored and enshrined in industry best practices and standards. Furthermore, global coordination is required to avoid regulatory arbitrage on technology development or implementation issues due to diverging regulatory requirements (e.g. data privacy rules).

- *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. AFME believes that an ongoing review of the technological architecture by regulators should be avoided. We believe that industry standards and best practices should be adopted and consist in of the following principles:

i) **Transparency**: allow adequate transparency to the user of the algorithm for inter-operability and simplified integration with legacy systems, transparency on the data used for data privacy issues;
ii) **Scrutiny**: on the model design, validations and testing in the context of established industry best practices beyond financial services;
iii) **Control**: allow user control of the data processed for data privacy concerns, of the path taken by the algorithm, of the potential outcomes (e.g. customer clustering/exclusion); adequate controls over undesired behaviours;
iv) **Training**: appropriate training should be considered to increase the understanding of the processing/functioning of the algorithm as well as the underlying business processes and interdependencies.

The industry could take precedent from other approaches such as risk/capital calculations, algorithmic trading where control approaches have been taken (e.g. "circuit breaker" ensuring algorithms operate within defined parameters). In other cases, the industry may use independent reviews to test and validate models used. In the specific case of AI, i.e. machine learning algorithms, existing controls will need to be adapted so they operate safely due to the non-static nature of algorithms (e.g. "learning").

Question 1.4:

- *What minimum characteristics and amount of information about the service user and the product portfolio (if any) should be included in algorithms used by the service providers (e.g. as regards risk profile)?*

  AFME believes that an ongoing review of the technological architecture by regulators should be avoided. We believe that industry standards and best practices should be adopted and consist in of the following principles:

  i) **Transparency**: allow adequate transparency to the user of the algorithm for inter-operability and simplified integration with legacy systems, transparency on the data used for data privacy issues;
  ii) **Scrutiny**: on the model design, validations and testing in the context of established industry best practices beyond financial services;
  iii) **Control**: allow user control of the data processed for data privacy concerns, of the path taken by the algorithm, of the potential outcomes (e.g. customer clustering/exclusion); adequate controls over undesired behaviours;
  iv) **Training**: appropriate training should be considered to increase the understanding of
  the processing/functioning of the algorithm as well as the underlying business
  processes and interdependencies.

Question 1.5:

- *What consumer protection challenges/risks have you identified with regard to artificial intelligence and big data analytics (e.g. robo-advice)?*

  AFME views that the challenges posed by these technologies may fall under the following categories:

  i) **Control**: Ensuring that the technology allows control over the outcome;
  ii) **Transparency**: Ensuring that the technology allows transparency on the outcome;
  iii) **Consumer protection**: Ensuring that the technology allows fairness of customer treatment.

  However, these challenges are not dissimilar to the challenges faced and managed by financial services today; although these may be exacerbated by the technology itself. Therefore, AFME believes that the technology should be explored further, with the active participation of various actors, to enshrine the appropriate design and controls required.

  Furthermore, with specific regards to big data, several existing EU legislations and/or other regulatory requirements, such as the Payment Services Directive 2

(PSD2), the General Data Protection Regulation (GDPR) and the Markets in Financial Instruments Directive (MIFID 2), are expected to mitigate potential risks which could be linked to the lack of transparency and misuse of data.

1.2. Social media and automated matching platforms: funding from the crowd

Question 1.6:

- *Are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding? In what way?*

Yes. AFME believes that national regulatory regimes are impacting the development of crowdfunding in Europe. Currently, the crowdfunding landscape is fragmented due to diverging national practices and disharmonised regulation, making the cost of raising capital higher in some Member States than in others.

More efforts could be made to develop early-stage finance in Europe which could be achieved by a harmonised landscape: addressing fragmented national crowdfunding frameworks, making use passporting regimes and ensuring a consistent regulation.
As well, the creation of a European single market for retail and semi-professional investors, would serve as a pan-European crowdfunding platform, operating across borders (under the EU's MiFID regulation), taking precedent over national legislations.

Furthermore, AFME believes the European Commission could consider reducing other barriers to crowdfunding such as national divergences in interpretation of the prospectus regulation, fiscal practices and company laws.

Equity crowdfunding platforms play an increasing role in providing funding to SMEs and start-ups. Funding amounts are in many cases between €500,000 and €1m[2] for securities-based crowdfunding in the main markets, with average amounts in the UK even higher. Providing an alternative source of funding, crowdsourcing, is a welcome development for the development of risk capital in Europe.

- *What are the critical components of those regimes?*

The European Crowdfunding Network (ECN) provides strong support to the crowdfunding industry, but more assistance is needed. Notably, there is a need for more education, training and certifications for investors and businesses. Education for retail investors, high-net worth individuals and family offices about the benefits of investing in small private companies and start-ups would also redirect investments.

[2] p15 - https://www.afme.eu/globalassets/downloads/publications/afme-highgrowth-2017.pdf

In addition, the adoption of best practices derived from experience in the market are needed to promote visibility and the security of equity crowdfunding as well as to unlock further cross-border investments.

Question 1.7:

- *How can the Commission support further development of FinTech solutions in the field of non-bank financing, i.e. peer-to-peer/marketplace lending, crowdfunding, invoice and supply chain finance?*

Currently, the crowdfunding landscape is fragmented due to diverging national practices and disharmonised regulation, making the cost of raising capital higher in some Member States than in others.

More efforts could be made to develop early-stage finance in Europe, which could be achieved by a harmonised landscape: addressing fragmented national crowdfunding frameworks, making use passporting regimes and ensuring a consistent regulation.

As well, the creation of a European-wide single market for regulation for retail and semi-professional investors, would enable the emergence of pan-European crowdfunding platforms, operating across borders (under the EU's MiFID regulation), taking precedent over national legislations.

Furthermore, AFME believes the European Commission could consider reducing other barriers to crowdfunding such as national divergences in interpretation of the prospectus regulation, fiscal practices and company laws.

Equity crowdfunding platforms play an increasing role in providing funding to SMEs and start-ups. Funding amounts are in many cases between €500,000 and €1m[3] for securities-based crowdfunding in the main markets, with average amounts in the UK even higher. Providing an alternative source of funding, crowdsourcing, is a welcome development for the development of risk capital in Europe.

Question 1.8:

- *What minimum level of transparency should be imposed on fund-raisers and platforms?*

The European Crowdfunding Network (ECN) provides strong support to the crowdfunding industry, but more assistance is needed. Notably, there is a need for more education, training and certifications for investors and businesses. Education for retail investors, high-net worth individuals and family offices about the benefits of investing in small private companies and start-ups would also redirect investments.

[3] p15 - https://www.afme.eu/globalassets/downloads/publications/afme-highgrowth-2017.pdf

In addition, the adoption of best practices derived from experience in the market are needed to promote visibility and the security of equity crowdfunding as well as to unlock further cross-border investments.

- *Are self-regulatory initiatives (as promoted by some industry associations and individual platforms) sufficient?*

  Self-regulated initiatives would benefit from additional EU support. AFME believes the EU should support a unified single market with common protection for retail and semi-professional investors. AFME views in addition to a unified European landscape around a single market for retail and semi-professional investors, the industry should promote for the safe use of this technology. Best practices could be derived from the experience gained and complement self-regulated Initiatives:

  i) **Level playing field**: ensure appropriate protections are considered to protect more vulnerable investors
  ii) **Proportionality**: rules should vary according to the size, risk profile and degree of vulnerability of investors
  iii) **Controls**: Promote general protection and awareness of risk, which could be facilitated by reporting tools and adequate insurance policies
  iv) **Transparency**: Promote a safe environment to favour adequate matching of risk appetite focused on knowledge, education, financial and technical literacy

1.3. Sensor data analytics and its impact on the insurance sector

Question 1.9:

- *Can you give examples of how sensor data analytics and other technologies are changing the provision of insurance and other financial services? What are the challenges to the widespread use of new technologies in insurance services? Are there already examples of price discrimination of users*

  AFME views sensor data analytics and, in general big data, as technologies that are changing the provision of financial services using new sources of data. These solutions may enable better risk scoring, efficiencies in pricing and providing better suited solutions to customer needs.

  For example, UBI Insurance (usage-based insurance) is an example of insurance setting where the premium is based on a user's behaviour. These products offer incentives to good behaviour and therefore reduce premium price but also improve the overall well-being of its customers.

The use and development of these imply new challenges such as the use of personal data, security and protection, regulatory compliance and avoiding non-discriminatory behaviours.

Question 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.)?*

AFME views that in general firms already differentiate between clients based on information. For example: trading with clients might imply tiering in categories A/B/C based on their relationship and business size, with each of these tiers different levels of servicing may be associated.

These methods are based on data, and the use of big data analytics, means that it is occurring at a larger scale. The possible risks of big data, and means by which those risks might be mitigated, will have to be addressed by increasing,

i) **Control**: Ensuring that the technology allows control over the outcome;
ii) **Transparency**: Ensuring that the technology allows transparency on the outcome;
iii) **Consumer protection**: Ensuring that the technology allows fairness of customer treatment.

1.4. Other technologies that may improve access to financial services

Question 1.11:
Can you please provide further examples of other technological applications that improve access to existing specific financial services or offer new services and of the related challenges? Are there combinations of existing and new technologies that you consider particularly innovative?

- AFME views a number of technological applications that may improve access to financial services:

i) **Quantum computing**: could increase the speed of computational power (by tapping into quantum physics) and the analysis of complex data. Key challenges may prevent its widespread use such as cyber security, encryption and propagation of systemic risks;
ii) **Distributed Ledger Technology**: may revolutionise the way financial information is recorded, stored, shared and distributed. Benefits include higher degrees of competitiveness, mobilizing capital faster and more securely across borders, all of which support the objectives of the European Commission under the Digital Single Market (DSM) and Capital Markets Union (CMU). However, key challenges may prevent the widespread use of the technology such as interoperability, implementation, cost, scalability,

speed and resilience. AFME believes these may be overcome by appropriate design and a rigorous governance model;

iii) **Big data:** may allow firms to use new sources of data previously unavailable providing higher quality analytics/insights. Productivity and revenue gains are expected via more efficient customer servicing. The combination of Big data with other types of technologies such as advanced analytics or artificial intelligence may yet increase its potential even further;

iv) **Robotics:** encompasses a wide range of technologies which emulates human intelligence processes. These technologies may provide significant gains by automating time consuming, prone to error, complex and difficult tasks. The combination of robotics with big data, advanced analytics, censor analytics and artificial intelligence may increase even further the potential of these technologies;

v) **Cloud technology:** may enable efficiency gains, by reducing the high costs of storage and processing of data, increasing scalability, and by connecting computational capabilities to a wider network of servers and specialist providers

2. BRINGING DOWN OPERATIONAL COSTS AND INCREASING EFFICIENCY FOR THE INDUSTRY

Question 2.1.

- *What are the most promising use cases of FinTech to reduce costs and improve processes at your company?*

Within wholesale banking, AFME views the following uses cases for FinTech:

i) **Cloud Technology**: "Private Clouds" provide developers with rapid agility, allowing for more time on developing as opposed to provisioning infrastructure and application services. "Public cloud" reduces peak infrastructure requirements by providing compute service scalability during temporary fluctuations in demand, reduces long-term storage costs and accelerates developer access to cloud services;

ii) **Robotics**: "Process automation" automates routine and manual intensive tasks, with 24/7 performance and reduction of human errors. "Machine learning" could provide more data insights by actively learning from data patterns. This may have positive impacts for the industry in areas such as loan servicing, where 80% of errors today occur due to errors in contract interpretation. "Cognitive automation" could automate more complex, human-like processes, such as perceiving, hypothesizing and reasoning, by combining "robotics" and "machine learning". For example, this could lead to virtual assistants that could respond to support service desk requests through a natural language interface;

iii) **Distributed Ledger Technology** in allowing,

a. Efficient information propagation: latest data is updated and replicated in close to real time;
b. Full traceability of information: new information is added to the ledger but not deleted creating an immutable chain of data where information is fully traceable;
c. Simplified reconciliation: mutualised information reduces reconciliation efforts;
d. Trusted disseminated system: data authenticity is completed by participants of the network rather than a central body;
e. High resiliency: the distributed nature of the information allows data to be recovered directly from any participant in case of local system failures.

- *Does this involve collaboration with other market players?*

Yes. AFME views positive effects in collaborating with other market players as the technology matures. While the industry is developing proof of concepts which may work in isolated situations, key challenges prevent widespread deployments, where economies of scale would be achieved. Therefore, we see collaboration with other market players as a positive step to increase investments and knowledge in the technology. The benefits of collaboration could extend beyond market players and include other actors of the eco-system, due to the inter-dependencies of financial services: vendors, third party providers, market infrastructures, regulators and international bodies (defined as eco-system thereafter).

Question 2.2.

- *What measures (if any) should be taken at EU level to facilitate the development and implementation of the most promising use cases? How can the EU play its role in developing the infrastructure underpinning FinTech innovation for the public good in Europe, be it through cloud computing infrastructure, distributed ledger technology, social media, mobile or security technology?*

AFME believes that the completion of European strategic objectives, such as the Digital Single Market (e.g. DSM) and Capital Markets Union (e.g. CMU), are key to create a globally innovative and integrated European capital markets, which will facilitate the development and implementation of FinTech.

Harmonising national regulatory and fiscal regimes, data protection laws and regulatory requirements, could reduce barriers to innovation. Furthermore, adopting a pan-European nurturing approach to innovation, such as the UK FCA's "Project Innovate", and facilitating collaboration amongst market players and others could increase technological developments.

AFME views the following initiatives at the EU level that would facilitate the development and implementation of the most promising uses cases:

i) **Promoting safety standards**: should be considered to ensure FinTech are designed and implemented with the required levels of security standards, for consumer protection, making them safe and resilient businesses;

ii) **Go-to market efficiency**: should be considered as a mean to accelerate the FinTech learning curve. This could be achieved by reducing the impact of pilot cost and enabling faster market access to gain customer feedback early on;

iii) **Harmonisation of practices**: are a key component to reduce the complexity of scaling up business. For example, AFME believes that the lack of a harmonised approach to outsourcing requirements prevents wider adoption of cloud computing. Furthermore, a unified framework for penetration testing is required to reduce efforts of organisation covering multiple geographies to comply with multiple versions of the same, as articulated in the penetration testing framework being developed by GFMA and AFME;

iv) **Adapting the regulatory framework**: is key to ensure the appropriate rules and controls are still applicable as the technology matures. For example, the development of DLT could potentially impact the way market infrastructures operate, therefore rules should be adapted to encompass potential role changes;

v) **Increasing global alignment**: adopting globally recognised standards defined by international bodies such as the FSB or IOSCO, will reduce the risk of seeing fragmentations in technology designs;

vi) **Facilitating knowledge transfer**: should be considered to increase the dialogue across sectors and regions, benefiting the overall EU FinTech industry from lessons learned. This may apply beyond European borders as FinTech is a global phenomenon;

vii) **Increasing training**: strive for the continuous improvements of educational standards for all actors in the eco-system. This could be achieved via tools allowing the safe testing of FinTech (e.g. sandboxes).

Question 2.3.

- *What kind of impact on employment do you expect as a result of implementing FinTech solutions? What skills are required to accompany such change?*

AFME believes that at this time it is difficult to determine what if any impacts new technologies will have on employment.

AFME believes that in the short term, there may be challenges in meeting the increasing demand for individuals with new skills, although in the long run these should reduce as the job market adapts and increases the skillsets able to accompany this digital transition.

2.1. RegTech: bringing down compliance costs

Question 2.4.

- *What are the most promising use cases of technologies for compliance purposes (RegTech)?*

AFME views that the most promising uses cases for RegTech would focus on helping firms achieve regulatory compliance and regulators identify what rules apply to whom and where (e.g. business processes impacted), noting that any solutions would need to be based on explicit regulatory definitions and expectations. Application of RegTech could include regulatory reporting, Know Your Customer/Anti Money Laundering (defined as KYC/AML thereafter) standards, surveillance (e.g. conduct risk, behaviour analytics, suitability), threats to resilience and financial stability (e.g. cyber-attacks).

The technologies that could best support these achievements are:

i) **Artificial Intelligence (AI)**: by using enhanced data analytics to achieve better interpretations of data, this technology could improve regulatory compliance. The technology could recognise data patterns and learn as the data is being analysed to help understand and interpret data correctly;
ii) **Distributed Ledger Technology (DLT)**: smart contacts could allow the transfer of client information held on a distributed ledger to downstream parties, improving the efficiency of client on-boarding;
iii) **Cloud computing (Cloud)**: could more readily provide a holistic view on transactions pertaining to a specific client. This may provide greater efficiency in resolving AML cases;
iv) In addition, specific **tools which favour collaboration** should be considered: such as regulatory sandboxes and open-API interfaces which allow for regulators, FinTech and market participants to self-serve in the consumption of data.

- *What are the challenges and what (if any) are the measures that could be taken at EU level to facilitate their development and implementation?*

The following measures could be warranted at the EU level to facilitate the development of RegTech:

i) **Harmonising regulatory regimes**: harmonised and explicitly defined regulations would provide more clarity in terms of regulatory requirements for cross-border trades;
ii) **Adherence to global standards**: would support a global approach to issues such as cyber security and reduce the potential fragmentations of the design of implementation of technology;

iii) **Favouring collaboration**: should be encouraged between market participants and other actors of the financial eco-system to apply lessons learned and best practices cross border and cross sector. Various mediums could be used to achieve this such as discussion groups, forums, incubators, sandboxes;

iv) **Innovation culture**: The success of the FinTech landscape in the UK demonstrates that the regulatory culture to innovation (e.g. FCA "Project Innovate") can make a significant difference to the willingness to innovate.

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

Question 2.5.

- *What are the regulatory or supervisory obstacles preventing financial services firms from using cloud computing services?*

AFME members are seeing the following obstacles to the adoption of cloud solutions in the EU:

i) **Regulatory harmonisation**: the current EU framework on outsourcing that would apply to cloud providers, could evolve to account for recent technological developments in risk management and harmonise practices across the EU. In addition, restrictions imposed by EU General Data Protection Regulation 2016/679 (defined as GDPR thereafter) on the processing of personal data could further limit the development of outsourcing solutions;

ii) **Fragmented practices**: the European Commission should continue to work closely with the European Union Agency for Network and Information Security (e.g. ENISA) and other organisations such as the FSB and ISOCO to ensure the harmonisation of practices for the free flow of data both within the EU and internationally. As commented by the European Banking Association (EBA)[4]:

   a. Inconsistencies in regulatory and supervisory frameworks form an additional barrier to institutions using cloud services;
   b. High level of uncertainty regarding supervisory expectations applied to outsourcing cloud service provider;
   c. Heterogeneity in supervisory expectations regarding technical security of cloud computing services;
   d. Principle-based regulatory frameworks in certain member states and the degree of technical requirements, do not provide clarity on current supervisory expectations in the EU to institutions with a cross-border presence.

- *Does this warrant measures at EU level?*

[4] EBA Link

AFME believes the European Commission could support the following measures:

i) **Clarity on risk management:** could be provided for the usage of cloud solutions, allowing market participants to focus on the appropriate controls and process to efficiently manage third party risks allowing wider adoption of the technology;
ii) **Increasing competition**: regulators should consider the appropriate incentives to increase competition to further democratise the technology. This would not only reduce the cost of the technology but offer a mitigation tool for single points of failure.

Question 2.6.

- *Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with?*

Yes. AFME believes that the current regulatory requirements imposed on its members to manage third party/vendor risk management, such as for cloud service providers, are sufficiently stringent to ensure minimum requirements are embedded in banks' processes today. These include the monitoring and management of risk, regulatory compliance and business continuity/resilience. However further could be achieved to ensure cloud service providers meet the regulatory standards imposed on market actors.

- *Should commercially available cloud solutions include any specific contractual obligations to this end?*

Commercially available solutions should consider the following recommendations to address concerns in the industry:

i) **Security standards** (e.g. cyber-resilience);
ii) **Business resilience** (e.g. business continuity);
iii) **Flexibility to integrate with other applications**: AFME members currently operate with a blend of legacy and newer IT applications;
iv) **Ease of integration with current processes** which meet the required controls for regulatory reporting and compliance;
v) **Ability to inter-operate** with other service providers or other applications.

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

Question 2.7.

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

Distributed Ledger Technology (DLT) as defined by ESMA[5] are "records, or ledgers, of electronic transactions. They are maintained by a shared or 'distributed' network of participants (so-called 'nodes') and not by a centralized entity". AFME views two distinguishing factors for DLT's:

i) **Information access is decentralized** (e.g. not logically centralized);
ii) **Transactions do not necessarily require trusted third parties**.

As outlined by SWIFT and Accenture in their 2016 report[6] DLT allow some key benefits for financials services:

i) **Efficient information propagation**: latest data is updated and replicated in close to real time;
ii) **Full traceability of information**: new information is added to the ledger but not deleted creating an immutable chain of data where information is fully traceable;
iii) **Simplified reconciliation:** mutualised information reduces reconciliation efforts;
iv) **Trusted disseminated system**: data authenticity is completed by participants of the network rather than a central body;
v) **High resiliency**: the distributed nature of the information allows data to be recovered directly from any participant in case of local system failures.

AFME views the following opportunities for financial markets enabled by DLT.

i) **More efficient post-trade processes**:
   a. For Clearing and Settlement: DLT could accelerate the clearing and settlement of securities, by potentially rending this process instantaneous. In this context, DLT could be adopted either as (1) an optimisation tool under the existing framework to combine trade confirmation, affirmation, allocation and settlement instruction generation into a single step, or (2) with substantial restructuring of the current framework in which market infrastructure providers (e.g. CCP's) would adopt new roles, where reconciliation, reporting and cash flow calculations would be eliminated;
   b. For Record of Ownership: DLT may facilitate the safekeeping and record-keeping of ownership of assets by maintaining a single "golden source" of record. It may also enhance transparency and

[55] https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf
[6] https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services

facilitate financial crime and compliance analysis by banks and regulators.

ii) **Enhanced reporting and supervisory functions**: by posting information to a DLT and providing regulator access, it ought to be possible to eliminate regulatory reporting activities, placing control over data enquiry directly in the hands of the regulator.

iii) **Greater availability and security**:
   a. Availability: the distributed nature of DLT has the potential to reduce single point-of-failure risk, if a node is inoperable the other nodes can continue the processing of transactions;
   b. Security: Encryption protocols offer higher degrees of security, although AFME believes that DLT adoption within the securities market should be based around a private and permissioned design, with adherence to a rigorous governance framework.

iv) **Reduced counterparty risk and enhanced collateral management**:
   a. Counterparty and Systemic Risk: A shared ledger could provide the benefits of a CCP for short-dated transactions without the need for an intermediary;
   b. Collateral Management: By reducing uncertainty and removing inefficiencies, DLT could be implemented using a common record of trading activities and valuations, leading to reduction of disputes, management costs and increasing the effective use of collateral.

v) **Costs reductions**: By providing a shared ledger between trading counterparties, DLT reduce costs associated with reconciliation activities.

AFME views the following other opportunities for a wider DLT enabled eco-system:

i) **Wide spread adoption**: adoption of DLT across other asset classes (e.g. cash, foreign exchange, derivatives), across all activities related to the trading of securities (e.g. issuance, asset servicing) and adopted by all market participants (e.g. FMI's, Central banks, Market infrastructures), would move the industry towards a real-time integrated execution for clearing and potentially reducing settlement cycles:

ii) **Enhancing KYC and AML processes**: Using digital client identifiers, smart contacts could allow the transfer of client information held on a distributed ledger to downstream parties, improving the efficiency of KYC and AML checks across the financial system.

The following proof of concepts[7] are currently being explored by the industry in the following areas:

[7] p53 – 58, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf

i) **Corporate records**: by using DLT for keeping track of securities ownership could reduce costs associated with the underwriting & tracking of ownership;
ii) **Corporate actions**: by using DLT to remove duplicative processes and reconciliations between participants (e.g, issuing company, investors, intermediaries);
iii) **Post-trading**: by using DLT for clearing, settlement and asset servicing, could allow for near real-time settlement reducing counterparty risk, compliance and audit risks;
iv) **Asset tokenisation**: by using DLT so that bilateral trades potentially no longer require the services of an FMI, reducing intermediation costs;
v) **Contract execution**: using smart contracts on a DLT, to manage the lifecycle of financial products, would automate the execution tasks such as trade confirmations, cashflow verifications, payments, events management, reducing operational costs and risks;
vi) **Loan syndication**: by using DLT as a common repository for data amongst multiple parties, the standard life cycle for syndicated loans emission could be significantly reduced by removing duplicative processes, currently taking weeks on average;
vii) **Repo transactions**: by using DLT for record keeping of repo transactions and the tokenization of collateral, would increase the transparency of collateral positions;
viii) **Short-term debt**: by using DLT to enhance the issue, trading, transferring and redeeming of short-term debt by standardizing and reducing transaction processing;
ix) **KYC/AML processes**: using DLT to streamline KYC/AML processes by i) sharing client information to simplify on-boarding ii) increased transparency for transaction surveillance iii) one source of data for all transaction records, simplifying surveillance;
x) **Digital ID's**: by using DLT to store a combination of identity factors and records validated by trusted third parties, could improve KYC controls and financial inclusion;
xi) **Improving funding processes**: by using DLT to provide transparency on upcoming payments leading to efficient gains for cash management in treasury activities;
xii) **Alternative financing**: by using DLT as a virtual, fully decentralized funding platform to provide funding to start-ups;
xiii) **Standardising securities processing and data records**: by using DLT to reduce Nostro breaks by having banks make payments based on ledger data;

Question 2.8.

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

AFME views the following challenges for the implementation of DLT solutions,

i) **Design Considerations**:
   a. Information access: maintaining appropriate controls for confidentiality and resilience, markets participants will have to design DLT around a private and permissioned network;
   b. Centralisation: some of the key processes, such as user authentication and upgrade of the infrastructure and protocol could be centralised. A trade-off will need to be resolved between decentralisation of processes and potential performance loss;
   c. Compliant by design: DLT would represent an opportunity to redesign IT systems, from the ground up, with a view of resolving confidentiality, integrity, availability and regulatory requirements.

ii) **Maturity**: DLT remains largely untested compared to technologies that are prevalent. Therefore, AFME believes DLT adoption is most likely to be incremental to optimise current processes, while the technology matures, becomes scalable, and is more widely adopted;

iii) **Inter-operability**: In the absence of interoperability incentives of moving to DLT will be reduced. To achieve interoperability globally the industry should consider the use of a universal standards for reference data, such as ISO 20022;

iv) **Cost of adoption**: DLT networks will be adopted in relation to their relative cost-efficiency. Truly "enterprise grade" resilience that matches standards currently achieved by legacy systems is not yet available. Furthermore, banks will have limited capacity to undertake a radical overhaul of their technology platforms whilst simultaneously facing major programs of work such as Dodd-Frank, MIFID2 and Brexit[8];

v) **Standardisation challenges**:
   a. Nomenclature: Currently there are no clear terminology standards in the industry leaving room for potential misalignments;
   b. Data standards: There is no convention for data standardisation amongst DLT networks posing interoperability challenges;
   c. Resilience: DLT should establish an overall enterprise grade architecture matching existing security and resilience standards, such as CPMI-IOSCO PFMI;
   d. Cooperation: industry best practices should be developed collaboratively and globally to ensure the universal adoption of the technology.

vi) **Technological challenges**: the technology will have to enable the ease of use for new entrants or scalability benefits will be difficult to achieve. Encryption could be outpaced by quantum computing. Searching information on a DLT may not be as efficient as traditional models;

vii) **Operational challenges**:

[8] http://www.pwc.co.uk/industries/financial-services/insights/planning-for-brexit-afme-study.html

a. Collaboration: due to its distributed nature, participants are due to collaborate more closely for data validations. Effective threat detection could require closer cooperation.
b. Resilience: a resilient governance framework would require a high degree of cooperation for the operation of the service, which may prove challenging due to the competitive nature of the industry;
c. Dependencies: DLT developments may be hampered by other dependencies, such as investor funding timelines, treasury funding, FX constraints, and other manual processes;
d. Data Privacy: on DLTs may prove challenging if different entities need to access the information stored. Reputational risks in case of a breach may lead to networks only allowing a subset of participants to use the network reducing scalability benefits;
e. Cyber-risks: the use of messaging between participants and potentially smart contracts may increase vulnerability to cyber-attacks and contagion risks;
f. Encryption: the creation and usage of encrypted public/private keys to protect the confidentiality of data of markets participants may prove challenging to implement;
g. Latency: Increasing the number of nodes may hamper latency thus rendering the technology unacceptable for certain activities such as high-volume trading;
h. Operational Risk: whilst reducing the risk of reconciliation breaks, the risk of an error, replicated amongst all participants could prove challenging.

viii) **Governance framework**: A governance framework for DLT would lie in its ability to drive adoption whilst striking the balance between rules allowing for speed of processing whilst maintaining appropriate controls for safety and financial stability.
a. Roles and responsibilities: As seen by the 2016 BIS report[9], a governance framework for DLT would have to consider the rights attached to each participant in the network such as (1) a system administrator acting as the gatekeeper controlling access to the system and providing certain specific services (2) the asset issuer permissioned to issue new assets (3) The proposer permissioned to propose updates to the ledger (4) The validator permissioned to confirm the validity of a state changes (5) The auditor permissioned to view the ledger but not make updates;
b. Vetting and approving participants: establish an accredited evaluation capability and an approval process that engages other network participants and relevant supervisors;

[9] http://www.bis.org/cpmi/publ/d157.pdf

c. Monitoring compliance: establish an accredited capability for the ongoing review of network participant compliance against the governance framework and oversight of any agreed remediation actions;
d. Enforcing standards: establish a compliance review board comprising network participant appointees, a tiered regime of sanctions that can be deployed against non-compliant network participants and ensuring network participants maintain within the jurisdictional reach of the governance model as a condition of membership;
e. Managing cross-border disputes: establish an independent arbitration panel and process to oversee disputes between network participants, and enshrine the legal enforceability of its decision within the rules of membership for each network participant;
f. Liability in the event of a cyber breach: Define, develop, and maintain a cyber resilience framework aimed at addressing current and emerging cyber threats, establish a cyber risk management capability, establish a cyber risk board amongst network participants;
g. Regulatory accountability: engage relevant supervisors to agree on a framework through which regulators will ensure accountability for the management of DLT functions.

ix) **Regulatory challenges**:

a. Approach: AFME would recommend an agnostic approach to regulating DLT, avoiding unintended constraints to the development of the technology and ensuring regulation stays relevant to market actors;
b. Collaboration: engagement of regulators in the early development of the technology would avoid that DLT takes an unacceptable path to regulators. Furthermore, cross-border applications of DLT will require global regulatory coordination to ensure these applications are developed in a safe way;
c. Regulatory endorsement: AFME believes that the ability to settle DLT transactions in central bank money is a key factor for adoption;
d. Role changes: regulators will have to consider adapting the existing regulatory framework in the context of potential market actors role changes;
e. Regulatory compliance: under the EU General Data Protection Regulation 2016/679 (GDPR) participants may exercise a 'right to be forgotten' which may prove challenging to implement on an immutable chain of data such as DLT;
f. Jurisdictional challenges: legal liability and enforcement measures may prove challenging across geographies without a clear governance framework;
g. Legal nature of DLT: the lack of clarity on territoriality and liability regarding a digital technology may add to the complexity of different legal requirements;
h. Authentication: a legal framework is required for DLT to become a unique and trusted source of immutable and authenticated data;

i. Validation of documents: For DLT to be enabled on securities market the recognition of record of ownership/proof of existence will have to devised and aligned globally
j. Financial instruments: Recognition is required for the legal validity of financial instruments used on DLT platforms by regulators and supervisors;
k. Smart contracts: territoriality and liability issues for smart contracts will have to be considered in the event of a breach of contract involving multiple parties.

Question 2.9.

- *What are the main regulatory or supervisory obstacles (stemming from EU regulation or national laws) to the deployment of DLT solutions (and the use of smart contracts) in the financial sector?*

AFME believes that the following are the key obstacles to be considered:

i) **Approach**: AFME would recommend an agnostic approach to regulating DLT, focusing on the application of DLT as opposed to its use, and noting potential uses are varied, thus remaining important that any regulatory approach does not implicitly limit the development of the technology;
ii) **Culture**: Favour a nurturing approach to innovation allowing firms to explore innovation in a safe and collaborative environment;
iii) **Collaboration**: engagement of regulators in the early development of the technology would avoid that DLT takes an unacceptable path to regulators. Furthermore, cross-border applications of DLT will require global regulatory coordination to ensure these applications are developed in a safe way;
iv) **Regulatory endorsement**: AFME believes that the ability to settle DLT transactions in central bank money is key factor for adoption;
v) **Role changes**: regulators will have to consider adapting the existing regulatory framework in the context of potential market actors' role changes;
vi) **Regulatory compliance**: under the EU General Data Protection Regulation 2016/679 (e.g. GDPR) participants may exercise a 'right to be forgotten' which may prove challenging to implement on an immutable chain of data such as DLT;
vii) **Jurisdictional challenges**: legal liability and enforcement measures may prove challenging across geographies without a clear governance framework;
viii) **Legal nature of DLT**: the lack of clarity on territoriality and liability regarding a digital technology may add to the complexity of different legal requirements;

ix) **Authentication**: a legal framework is required for DLT to become a unique and trusted source of immutable and authenticated data;
x) **Validation of documents**: For DLT to be enabled on securities market the recognition of record of ownership/proof of existence will have to devised and aligned globally;
xi) **Financial instruments**: Recognition is required for the legal validity of financial instruments used on DLT platforms by regulators and supervisors;
xii) **Smart contracts**: territoriality and liability issues for smart contracts will have to be considered in the event of a breach of contract involving multiple parties.

2.4. Outsourcing potential to boost efficiency

Question 2.10.

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

Yes. While the current regulatory frameworks[10,11] for outsourcing are in AFME's view sufficient for mitigating challenges on risk management and implementing appropriate controls for managing third party providers, they also prove to be challenging in certain ways.

AFME members have been using outsourcing via third party providers such as FinTech to:

i) **Optimise their cost structure** (e.g. rationalising activities);
ii) **Increasing their revenues** (e.g. accessing new markets, servicing clients better).

Offshoring offers the opportunity to use outsourcing as a means to take advantage of relatively lower costs of labour in other geographies, which may be outweighed by inflationary pressures and other costs involved (e.g. infrastructure, training, oversight, attrition).

AFME supports the adoption of industry best practices for outsourcing arrangements, for example as referenced in the investment association's analysis[12]:

i) **Oversight**: 1) "Know Your Outsourcer" to design an outsourcing model, 2) perform a risk based assessment of outsourced arrangements, 3) establish an appropriate level of a senior ownership for the outsourced activity, iv) establish an appropriate oversight framework;

[10] http://www.bis.org/publ/joint12.htm
[11] https://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf
[12] https://www.theinvestmentassociation.org/assets/files/industry-guidance/20161121-OWGReport.pdf

ii) **Exit Planning**: 1) create a comprehensive exit plan, 2) embed the plan in the oversight framework, 3) perform periodic plan reviews, 4) complete a single approach exit plan, 5) documenting in detail key exit plans, 5) consider end-to-end transition planning, 6) frame the governance overseeing the transition;

iii) **Standards for**: 1) documentation of the operating model, 2) definition and identification of critical and non-critical data and functions, 3) testing methodology for due diligence reviews;

iv) **Operational strategy**: Firms should consider outsourcing solutions in the context of business model optimisation to, 1) gain efficiency by releasing costs through economies of scale, 2) increasing effectiveness by simplifying transactional activities to focus on value added activities, 3) manage operational risk better by spreading operations across locations to increase business continuity, 4) gain agility by enabling standardized, scalable and specialized solutions, 5) increase quality of service by enabling specific talents and processes, to establish domain specialization, 6) increase capital efficiency by releasing capital through efficient and effective sourcing.

We also note that as the current regulatory framework on outsourcing was established in 2006,[13] we believe that there is further opportunity to review and harmonise considering recent technology developments and their potential impacts on the industry. We note that national regulators have issued guidelines and recommendations on outsourcing which has led to a fragmentation of the European landscape: see guidelines issued by BaFin[14], Autorite des Marches Financiers (AMF)[15], Luxembourg for Finance[16] or the Central Bank of Ireland (CBI)[17].

The European Commission should work closely with national regulators to harmonise outsourcing practices providing more clarity on outsourcing requirements. Furthermore, collaboration with other regulators and international bodies (e.g. BIS, IOSCO, FSB) should be encouraged to converge these practices globally.

Question 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.*

[13] http://www.mifidconnect.com/mifidconnect/downloads/MiFID_Connect_Outsourcing_Guide.pdf
[14] BaFin Outsourcing Link
[15] AMF Outsourcing Link
[16] Luxembourg for Finance Outsourcing Link
[17] CBI Outsourcing Link

Yes. The current regulatory frameworks[18,19] for outsourcing are in AFME's view sufficient for mitigating challenges on risk management, and implementing appropriate controls for managing third party providers. However further effort is required to ensure they strike the appropriate balance between managing risks and allowing firms to take advantage of outsourcing as suggested by the adoption of industry best practices detailed further below.

AFME members have been using outsourcing, via third party providers such as FinTech to:

i) **Optimise their cost structure** (e.g. rationalising activities);
ii) **Increasing their revenues** (e.g. accessing new markets, servicing clients better).

Offshoring offers the opportunity to use outsourcing as a means to take advantage of relatively lower costs of labour in other geographies, which may be outweighed by inflationary pressures and other costs involved (e.g. infrastructure, training, oversight, attrition).

AFME supports the adoption of industry best practices for outsourcing arrangements, for example following the investment association's analysis[20]:

i) **Oversight**: 1) "Know Your Outsourcer" to design an outsourcing model, 2) perform a risk based assessment of outsourced arrangements, 3) establish an appropriate level of a senior ownership for the outsourced activity, iv) establish an appropriate oversight framework;
ii) **Exit Planning**: 1) create a comprehensive exit plan, 2) embed the plan in the oversight framework, 3) perform periodic plan reviews, 4) complete a single approach exit plan, 5) documenting in detail key exit plans, 5) consider end-to-end transition planning, 6) Frame the governance overseeing the transition;
iii) **Standards for**: 1) documentation of the operating model, 2) definition and identification of critical and non-critical data and functions, 3) testing methodology for due diligence reviews;
iv) **Operational strategy**: Firms should consider outsourcing solutions in the context of business model optimisation to, 1) gain efficiency by releasing costs through economies of scale, 2) increasing effectiveness by simplifying transactional activities to focus on value added activities, 3) manage operational risk better by spreading operations across locations to increase business continuity, 4) gain agility by enabling standardized, scalable and specialized solutions, 5) increase quality of service

[18] http://www.bis.org/publ/joint12.htm
[19] https://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf
[20] https://www.theinvestmentassociation.org/assets/files/industry-guidance/20161121-OWGReport.pdf

by enabling specific talents and processes, to establish domain specialization, 6) increase capital efficiency by releasing capital through efficient and effective sourcing.

We also note that as the current regulatory framework on outsourcing was established in 2006,[21] we believe that there is further opportunity to review and harmonise to consider recent technology developments and their potential impacts on the industry. We note that national regulators have issued guidelines and recommendations on outsourcing which has led to a fragmentation of the European landscape: see guidelines issued by BaFin[22], Autorite des Marches Financiers (AMF)[23], Luxembourg for Finance[24] or the Central Bank of Ireland (CBI)[25].

The European Commission should work closely with national regulators to harmonise outsourcing practices providing more clarity on outsourcing requirements. Furthermore, collaboration with other regulators and international bodies (e.g. BIS, IOSCO, FSB) should be encouraged to converge these practices globally.

2.5. Other technologies that may increase efficiency for the industry

Question 2.12.

- *Can you provide further examples of financial innovations that have the potential to reduce operational costs for financial service providers and/or increase their efficiency and of the related challenges?*

AFME views the following other examples of innovation that have key implications for cost reductions and efficiency increases in the industry:

i) **Cloud Technology**: "Private Clouds" provide developers with rapid agility, allowing for more time on developing as opposed to provisioning infrastructure and application services. "Public cloud" reduces peak infrastructure requirements by providing compute services during temporary fluctuations in demand, reduces long-term storage costs and accelerates developer access to cloud services;

ii) **Robotics**: "Process automation" automates routinely and manual intensive tasks, with 24/7 performance and reduction of human errors. "Machine learning" could provide more data insights by actively learning from data patterns. This may have positive impacts for the industry in areas such as loan servicing, where 80% of errors today occur due to errors in contract interpretation. "Cognitive automation" could automate more complex, human-like processes, such as perceiving, hypothesizing and reasoning, by combining "robotics" and "machine

[21] http://www.mifidconnect.com/mifidconnect/downloads/MiFID_Connect_Outsourcing_Guide.pdf
[22] BaFin Outsourcing Link
[23] AMF Outsourcing Link
[24] Luxembourg for Finance Outsourcing Link
[25] CBI Outsourcing Link

learning". For example, this could lead to virtual assistants that could respond to support service desk requests through a natural language interface;

iii) **Distributed Ledger Technology** in allowing,
   a. Efficient information propagation: latest data is updated and replicated in close to real time;
   b. Full traceability of information: new information is added to the ledger but not deleted creating an immutable chain of data where information is fully traceable;
   c. Simplified reconciliation: mutualised information reduces reconciliation efforts;
   d. Trusted disseminated system: data authenticity is completed by participants of the network rather than a central body;
   e. High resiliency: the distributed nature of the information allows data to be recovered directly from any participant in case of local system failures.

3. MAKING THE SINGLE MARKET MORE COMPETITIVE BY LOWERING BARRIERS TO ENTRY

Question 3.1.

- *Which specific pieces of existing EU and/or Member State financial services legislation or supervisory practices (if any), and how (if at all), need to be adapted to facilitate implementation of FinTech solutions?*

AFME agrees with the recommendations outlined by the European Banking Federation (EBF) in its paper on banking in the Digital Age[26] to:

i) **Develop digital financial services** by recommendations and legislative proposals;
ii) **Ensure a level playing field** between different types of providers.

Additionally, we believe that there is further need to develop efficient and secure remote identification (eID) systems that can be used by the financial sector to connect with its clients. In this regard, national eID systems should be interoperable and accessible for the private sector to verify the identity of digital customers. The Electronic Identification and Trust Services Regulation (eIDAS Regulation) creates an interoperability framework for the national eID systems to be recognized by public bodies across the EU. However, the framework leaves it to Member States to define the terms of access to the online authentication of eIDs for the private sector. This gap should be addressed by creating a clear framework for the private sector to use national eID systems, clearing out the liabilities in case of vulnerabilities, misuse, fraud, cyber-attacks on entities acting as the central identity holder.

[26] http://www.ebf-fbe.eu/wp-content/uploads/2016/11/EBF_024052-Press-release-EBF-Vision-for-Banking-in-the-Digital-Single-Market.pdf

Finally, we agree that there is a need to update the regulatory and supervisory framework on outsourcing and adapt it to cloud technology. The European Commission should work closely with the EBA to collect the feedback received on its 2017 public consultation on cloud technology, which we believe could add value to any updates of the EBA's current guidance on cloud outsourcing.

AFME agrees that there is a need to harmonize the criteria followed by national supervisors when approving cloud projects. The European Commission should consider bringing forward EU ex-ante guidelines for the use of cloud projects which would provide greater adoption of these services and streamline national requirements. The industry would aspire to have pre-approved contracts with the identified providers for specific types of initiatives.

Question 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?*

AFME views the EU FinTech ecosystem as strong and growing with the current levels of regulatory engagement. As this ecosystem continues to evolve, regulators should monitor emerging risks and engage when warranted, while ensuring there are no constraints on collaboration within the ecosystem. Engagement beyond this may have unintended consequences.

AFME would caution the European Commission in its approach towards financial innovations due to the proven benefits in improving the quality and variety of banking services.

Innovation has a high degree of uncertainty due to the risks involved, including maturing technologies, low levels of prior experience (regulators and market participants alike) and new legal requirements. Therefore, authorities should actively seek tools to reduce regulatory ambiguity by establishing collaboration channels with the industry and facilitate dialogue between banks, nonbank FinTech, regulators on:

i) **the barriers** to partnerships;
ii) **the marketing** of innovative services/technologies.

3.1. Role of regulation: licensing, proportionality and outsourcing

Question 3.3.

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

  AFME believes that a more harmonised approach towards innovation in Europe would be beneficial to its development. The regulatory barriers created by a fragmented regulatory landscape results in innovators finding it more difficult to scale up due to the lack of clarity on regulatory requirement once moving across borders.

  AFME encourages the European Commission to work closely with innovation hubs, industry actors, consumers, vendors, other regulators and industry bodies to work on reducing uncertainty for the FinTech landscape.

  Question 3.4.

- *Should the EU introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market? 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?*

  AFME cannot comment on this question due to the lack of specific details on the licensing categories and would be happy to provide further commentary at a later time. However, we feel that clear and comprehensive regulatory and supervisory framework should be provided before introducing a new license for FinTech activities. To this end, and in light of the Commission's recently published CMU Mid-Term Review[27], in which the Commission commits to assessing the case for an EU licencing and passporting framework for FinTech activities in Q4 2017. AFME recommends that the Commission undertakes a public consultation with regards the issue.

  Question 3.5.

- *Do you consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market? If so, please explain in which areas and how should the Commission intervene.*

  Yes. AFME views that further action is required for proportionality in financial services and this should be considered under the lens of individual risks created, not only a firm's size.

[27] p.13 - https://ec.europa.eu/info/sites/info/files/communication-cmu-mid-term-review-june2017_en.pdf

AFME believes that European regulations should focus on how to best manage stability, integrity and consumer protection risks.

Question 3.6.

- *Are there issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market?*

AFME views that restrictions on the flow of data could affect the Digital Single Market.

While data localisation measures may be justified in limited circumstances (e.g. confidential government data), their impact on the growth of the European data economy is negative: they fragment the single market and raise costs for the deployment of cross-border data economy services.

Such measures have an impact on the infrastructure underlying the data economy – such as cloud services – because these services require major investments which cannot feasibly be made on a country-by-country basis.

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

Data localisation regulation and restrictions on data movement take many forms including specific regulations, certification/accreditation, administrative requirements, procurement policies, and regulatory guidance, many of which are sector-based. The impact of data localisation on cross-border transactions is significant. Data localisation adds to the complexity of cross-border business strategies and restricts market access.

Question 3.7.

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

Yes. AFME views that the three principles are appropriate.

3.2. Role of supervisors: enabling innovation

Question 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?*

AFME believes the European Commission and ESA's should continue to leverage the following efforts:

i) **Tailored and responsive regulation**: financial regulation should benefit from technological improvements, regulation should neither stifle innovation nor prevent sound and safe competition. AFME believes the EU should therefore foster an agile, proportionate and effectiveness-oriented regulation of Fintech and financial innovation;
   a. Agile regulation: regarding the emergence of new technologies and new business models, regulatory adjustments could be contemplated (including regulatory simplifications) and new status could be introduced, focusing on the main risks raised by the activity (e.g. crowdfunding regulation in France[28]). Agile regulation could also be promoted by "test and learn" initiatives. For example, the French law acknowledges blockchain technology for the register on non-listed equities. Based on that first live experiment, blockchain technology could later be acknowledged for an extended scope of services;
   b. Proportionate: regulation and supervision should always be proportionate and driven by considerations of risk scale (consumer protection and AML/CFT mainly, financial stability if FinTech eventually gain significant market shares). This philosophy allows softening regulatory scope entry. Oriented towards effectiveness: rather than being too prescriptive or detailed, principle-based regulation is likely to be more effective and more adequate in very innovative environments.

ii) **Participation should be voluntary** for established financial institutions, as there are already robust controls and risk management processes in place.

- *Question 3.9. Should the Commission set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns? If yes, please specify how these programs should be organised?*

  Yes. AFME views benefits in establishing an "Innovation Academy" and would welcome supporting the establishment of such an initiative. We believe this could help centralise efforts related to the development of a FinTech in a safe and coordinated environment:

[28] http://www.amf-france.org/en_US/Acteurs-et-produits/Prestataires-financiers/Financement-participatif---crowdfunding/Cadre-reglementaire

i) **Cross border and cross sector learning**: could derive benefits for the use of Fintech to a broader range of stakeholders. For example, by learning best practices for the running of FinTech projects based on case studies. These could be applied to a multitude of topics such as how to correctly use new technologies and forecasting trends;

ii) **Appropriate representation**: should be considered to drive conversations. These could include industry actors, consumer associations, academics researchers, regulators, vendors, third-party providers, non-for-profit. Furthermore, due to its potential scope representation from other international bodies should be considered, in particular other regulators in order to address issues globally;

iii) **Identification of the "areas of focus"** for this an Innovation Academy would help identify the appropriate actors to involve at an early stage and ensure appropriate representation.

Question 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?*

AFME suggests that harmonised coordination between Member States may be a more successful model rather than trying to establish a single European level sandbox.

Question 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.*

AFME is not responding to this question.

3.3. Role of industry: standards and interoperability

Question 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?*

AFME believes that further efforts are required. The increasing role and development of technology in the delivery and management of financial services should increase requirements on interoperability and standardisation. Authorities should foster and support standardization initiatives by market players and focus on solving overlaps between different regulations.

Strong standards allow technology and financial services providers to develop their products and services that can integrate and interact with the broader financial infrastructure, and should consider:

i) **Standardisation should be competition-friendly**: participation in standard-setting should be unrestricted, procedures for adoption of standards should be transparent and access to standards should be granted on fair, reasonable and non-discriminatory terms to prevent foreclosure of new entrants;
ii) **Market efficiency** could be impaired by fragmented processes and lack of standardisation;
iii) **Harmonisation, development and adoption of standards** should be a basic building block for achieving interoperable services.

AFME views that standardisation would foster competition and interoperability on the "standardised" activities, as long as these standards do not hinder innovation and ensure a level playing field, among FinTechs and established Financial Institutions.

Question 3.13.

- *In which areas could EU or global level standards facilitate the efficiency and interoperability of FinTech solutions?*

AFME views the adoption of global standards as key to the development of FinTech given the global essence of technology. Global international standards, recognized by the industry, should be best placed to foster not only efficiency and interoperability but also competition and ensuring a global level playing field. To ensure adoption, efficiency, interoperability and avoid these standards being artificially imposed, standards initiatives should be left to the willingness and involvement of market participants.

- *What would be the most effective and competition-friendly approach to develop these standards?*

The most effective and competition-friendly approach to developing these standards should be for new regulatory and supervisory frameworks, addressing FinTech innovation, to be harmonious with existing innovation frameworks. This would mitigate against conflicting rule sets that could inhibit the development of innovative products and services.

As global regulatory bodies (FSB/IOSCO/Basel) continue to monitor this space, they should help coordinate FinTech-focused policies from member jurisdictions such as the EU.

Question 3.14.

- *Should the EU institutions promote an open source model where libraries of open source solutions are available to developers and innovators to develop new products and services under specific open sources licenses? What other specific measures should be taken at EU level?*

  Yes, AFME believes EU institutions should support a framework that would allow open source models to flourish, leaving the implementation of specific use cases to willing market initiatives.

  Open source models offer key benefits for both users and developers. They offer an alternative to proprietary software and valuable features, such as the ability to adapt, and more specialised tailoring by enhancing the application and the ability to verify models against peers.

3.4. Challenges: Securing financial stability

Question 3.15.
How big is the impact of FinTech on the safety and soundness of incumbent firms? What are the efficiencies that FinTech solutions could bring to incumbents? Please explain.

While it is difficult to quantify the impact of Fintech, AFME believes that a number of benefits have already materialised with a view to financial stability. We also believe that as previously mentioned efficiencies will be gained through increased automation, transparency and better valued propositions to customers.

4. BALANCING GREATER DATA SHARING AND TRANSPARENCY WITH DATA SECURITY AND PROTECTION NEEDS

Question 4.1.

- *How important is the free flow of data for the development of a Digital Single Market in financial services?*

  AFME views as essential the free flow of data for the development of a Digital Single Market. It should allow the further unlocking of the benefits of Fintech by digitally transforming financial services.

  Free flow of data should be accompanied with appropriate controls and processes to safeguard against cyber-attacks, address privacy concerns and protect personal/sensitive data. This could be achieved by embedding appropriate controls from the early design stage (e.g. governance and transparency) and implemented consistently by ensuring collaboration of all actors of the eco-system, at a global level.

In addition, the EU should be particularly wary of the challenges posed by a potentially fragmented digital landscape and work towards increasing harmonisation and collaboration. Such as the transposition of the NIS[29] directive in national law.

AFME considers that data protection legislation appropriately restricts service providers from processing data of service users for purposes that go beyond the purposes for which the data was collected (purpose limitation). This is an adequate protection for service users.

- *Should service users (i.e. consumers and businesses generating the data) be entitled to fair compensation when their data is processed by service providers for commercial purposes that go beyond their direct relationship?*

In the processing of personal data by service providers for commercial purposes, AFME views that end users may benefit from an enhanced customer service within existing data privacy regulations.

4.1. Storing and sharing financial information through a reliable tool

Question 4.2.

- *To what extent could DLT solutions provide a reliable tool for financial information storing and sharing?*

AFME believes that DLT could offer a reliable tool for storing and sharing information, including financial information.

DLT offers opportunities for information sharing due to inherent characteristics such as encryption, distribution, replicability, immutability and consensus validation. As such, DLT offers key benefits for data distribution as participants can self-service and information is replicated across the network.

Key considerations would have to be considered and addressed, should DLT technology become a widespread platform for storing and sharing financial data.

DLT design considerations related to a permissioned and private network are viable options for financial services data. Careful data partitioning and encryption will be key for data privacy considerations. A strong governance framework and the active collaboration of all actors of the eco-system would be required to ensure inter-operability and resilience against external threats.

- *Are there alternative technological solutions?*

[29] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

AFME believes alternative technologies are available for the storing and sharing of financial information, which could achieve the same purpose, such as APIs, advanced messaging services and microservices.

The industry could as well invest in further enhancing legacy platforms which have proven track records in testing and resilience. However, rather than building solutions on legacy technology, DLT based solutions offer added value. A single consolidated report would be beneficial, to avoid having to receive and consolidate reports from individual contributors, offering potentially real-time record access to Regulators.

Question 4.3.

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

We believe that further efforts are required, and digital identities should be further developed as they are critical enablers for deriving some of the key benefits of FinTech.

This is particularly true for financial services transactions where the authentication of actors is a key enabler of trust. Digital identities would as well be essential for the prevention of financial crime (e.g. fraud, money laundering, cyber-attacks) and would support efforts and regulation encompassing KYC/AML processes to date.

AFME is supportive of the European Commission's initiatives under the creation of a Digital Single Market such as eIDS and eTS[30].

The European Commission should engage with other regulators to benefit from the lessons from the following on-going initiatives,

i) **The Monetary Authority of Singapore** (MAS) is piloting a national know-your-customer (KYC) utility for financial services, based on the MyInfo digital identity service[31];
ii) The Hong Kong Monetary Authority (HKMA) and Applied Science and Technology Research Institute (ASTRI) have formed a Digital ID Working Group with five participating banks to study the feasibility of applying DLT to digital identity management[32];
iii) **The Aadhaar program**, kicked-off in 2009 by the Government of India, through the Unique Identification Authority of India (UIDAI), launched an ambitious biometric identity program;

[30] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
[31] https://www.tech.gov.sg/Media-Room/Media-Releases/2017/05/Opening-Bank-Accounts-Becomes-More-Seamless-and-Convenient-for-MyInfo-Users
[32] http://www.hkma.gov.hk/eng/key-information/press-releases/2016/20161216-3.shtml

iv) **The Sovrin Foundation has initiated "Project Indy**"[33] to create under the Hyperledger DLT platform a form of simple private identity or Self-Sovereign Identity (SSI), 100% owned and controlled by an individual or organization;
v) **The "GSMA Mobile Identity programme**"[34] aims to help digital service providers and consumers find the optimum balance between privacy, security and convenience;
vi) **The IBM and SecureKey Technologies initiative** aims at delivering a blockchain based Digital Identity network for consumers[35].

Further efforts to encourage i) the creation a common framework to avoid fragmentation of practices and regulations across European counties, ii) the creation of proofs-of-concepts which may support progress on concrete initiatives, may support better adoption of digital identities.

We would also like to note a certain number of challenges which will have to be addressed to enable the full benefits of digital identities to be achieved:

i) **Financial exclusion**: while digital identities could support the reduction of financial exclusion (e.g. access to financial services) actors would have to consider what needs to be done for individuals who do not have access to a computer or a mobile device;
ii) **Authentication**: actors will have to consider what characteristics are required to fully authenticate individuals and legal entities for financial transactions such as "multi factor authentications" using a combination of factors: proofs of identity, biometric data and trusted third parties;
iii) **Identity fraud**: while encryption offers useful tools to prevent identity fraud, regulators and processes would have to adapt to the new challenges posed by digital identities;
iv) **Infrastructure**: due to the sensitive and personal nature of digital identity data, actors will have to consider what would be the appropriate infrastructures to host this information;
v) **Interoperability**: with digital identities arising from local initiatives and using a multitude of different technological supports, such as DLT, actors will have to consider what interoperability means between different solutions, in particular for actors operating globally;
vi) **Adapting regulation**: regulators will have to adapt their roles and regulations to cater for the needs of this new environment.

Question 4.4.

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

[33] https://www.sovrin.org/
[34] https://www.gsma.com/identity/
[35] https://www-03.ibm.com/press/us/en/pressrelease/51841.wss

AFME views that the challenges for using DLT with regards to personal data protection are linked to its characteristic as an immutable chain of data which could pose challenges with "the right to be forgotten" under GDPR.

These challenges may be overcome by the partitioning of data, encryption technics or even the use of a potential EU infrastructure for storing personal data, such as digital identities, which would be compliant by design.

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

Question 4.5.

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

AFME suggests that financial service providers are constantly investing into tools and methods that would enable them to make sounder investment decisions (e.g. managing their balance sheet) such as risk profiling.

This is a required competence at the core of the banking system, inherently linked to its role as a financial service provider.

Big Data and AI may provide enhanced risk profiling models by capturing more data points than currently available tools which could enable:

i) **More revenue opportunities by**: increasing capital allocations to areas previously excluded
ii) **Better customer servicing (consumers and SME's) by**: providing a broader range of products (comparative tools & product aggregators), tailoring products and advice (e.g. improved credit scoring, increasing product suitability) and reducing risks (e.g. rigorous audits trails)

AFME views that a critical condition for the delivery of these benefits will depend on data quality. If data is unreliable then results might not be accurate.

Question 4.6.

- *How can counterparties that hold credit and financial data on SMEs and other users be incentivised to share information with alternative funding providers ? What kind of policy action could enable this interaction? What are the risks, if any, for SMEs?*

Financial services are held to strict data protection and customer confidentiality requirements, which restrict them from sharing information on their customers with third parties, whether SMEs or other categories of customers.

Tools such as Open API's, Sandboxes, Data encryption/anonymisation, industry forums to share best practices and standards may offer useful means to share information in a compliant format.

AFME believes that information sharing that is pertinent to the promotion of financial stability should be more broadly disseminated such as intelligence sharing for cyber-attacks or financial crime.

4.3. Security

Question 4.7.

- *What additional (minimum) cybersecurity requirements for financial service providers and market infrastructures should be included as a complement to the existing requirements (if any)? What kind of proportionality should apply to this regime?*

AFME believes that the current requirements under the Directive on Security of Network and Information Systems (e.g. NIS) are positive steps for tackling the ever-growing cyber security threat, as seen in the most recent global attack of the WannaCry ransomeware[36]. While the directive looks into enhancing cross-border cooperation in case of a major cyber-incident more efforts are required.

AFME believes cyber security requires global coordination to address any threats. The European Commission should work closely with its national regulators, ENISA, industry actors, vendors and organisations to ensure coordination and harmonisation is achieved across borders.

Furthermore, the EU should work closely with internal bodies such as the G20, FSB or IOSCO to coordinate efforts and harmonise practices globally.

AFME is partnering its sister organisation, the GFMA, to develop a penetration testing framework, which is required to enable consistency and good practice for Regulatory sponsored implementations of 'Red team'[37] testing. If this is not achieved, it will result in the implementation of multiple regional penetration testing requirements, which we believe will lead to operational risk and operational overhead to complete multiple 'Red Team' tests.

The framework has been designed with a view that Regulators can place reliance on 'Red Team' testing activity performed by other Regulators reducing the need for additional tests to be run.

The European Commission should consider the following recommendations:

ii) **Harmonising cyber hygiene requirements** on:

[36] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[37] https://www2.deloitte.com/nl/nl/pages/risk/solutions/red-teaming-operations.html

a. Controls: the appropriate mapping of an IT infrastructure, passing credentials securely, version patching, infrastructure dependencies (e.g. to third-party providers), compartmentalisation and segregation of applications;
b. Readiness in case of an attack: mapping of critical assets, organisational dependencies for taking fast and effective decisions, scenario building.

iii) **Harmonising critical infrastructure penetration testing**: due to the specific skills required for 'Red team' testing AFME encourages the development of credentials that may certify the skills required (e.g. identify threats without disrupting potentially live systems);

iv) **Increasing information sharing**: intelligence and information sharing play a key role in the prevention of cyber-attacks, the European Commission should consider how firms may continue to share data to prevent cyber-attacks. Currently under GDPR, the sharing of IP Addresses may be prevented due to its tie with personal data[38].

The European Commission should work closely with efforts supported by global supervisors on risk-based approaches to cybersecurity risk management. Adoption of the G7 "Fundamental Elements of Cybersecurity for the Financial Sector" should be considered as a starting point for all cybersecurity regulation and the NIST framework should be considered as an example of an instantiation of the principles defined in the G7 "Elements".

Question 4.8.

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

AFME believes that information sharing for the purpose of security, financial stability in the event of fraud, financial crime or cyber-attack detection would benefit the financial system at large.

In an interconnected environment early detection, prevention and adequate protection are key attributes for the security and stability of the system.

The view 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. Industry players have been engaging in information sharing and coordinated analytics work in this space.

AFME sees positive support from the European Commission in tackling cyber-attacks via the NIS directive but there could still be fragmentation in the way the

[38] http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

directive is transposed in local countries. AFME supports a consistent approach to the implementation of NIS directive.

Whilst embracing the required needs for personal data protection, AFME believes the European Commission should carefully consider the unintended consequences of GDPR. The potential impact of GDPR on the processing of personal data, such as IP addresses and the right to erasure (which could be instrumental evidence in a criminal investigation procedure) may add further complexity in managing cyber risks.

Question 4.9.

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

Penetration testing led by third parties introduces operational and data risks. AFME is supportive that firms conduct their own penetration tests in partnership with regulator, based on the framework AFME and the GFMA are developing.

AFME is supportive of a safe and scalable approach to regulatory penetration testing and "Red team" testing across the entire EU, where single test results satisfy multiple supervisors' requirements (limiting the operational risk execution of penetration tests or "Red team" assessments).

4.4. Other potential applications of FinTech going forward

Question 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?*

Apart from those examples previously discussed, AFME believes that the free flow of data, by allowing clients to share with financial services providers their personal data in the hands of other firms, may reduce information asymmetries and improve access to financial services. Greater access to clients' data may improve creditworthiness assessments and increase access to credit.
AFME's view is the regulatory requirements for data sharing and transparency should continue to be technology agnostic and focus on usage and outcomes.