EFAMA Response to EC Consultation Report on FinTech

EFAMA is the representative association for the European investment management industry. EFAMA represents - through its 28 member associations and 62 corporate members - close to EUR 23 trillion in assets under management, of which EUR 14.1 trillion managed by 58,400 investment funds at end 2016. Just over 30,600 of these funds are UCITS (Undertakings for Collective Investments in Transferable Securities) funds, with the remaining 27,800 funds being AIFs (Alternative Investment Funds).

We appreciate the opportunity to respond to this important consultation and remain gladly at the disposal of the European Commission staff to elaborate on any of our responses.

Section I - Fostering access to financial services for consumers and businesses

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

In broad terms, with a view across the asset management industry as a whole, the following are the main FinTech applications being developed in light of their potential to gradually transform existing practices in terms of:

(i) Initial client on-boarding and following interactions, with or without the intervention of a human advisor ("automated advice");

(ii) Automating front- to back-office functions (via distributed ledger technology or "DLT", "smart contracts", robotic process automation or intelligent algorithms)[1];

(iii) Using artificial intelligence to complement fundamental analysis in the investment process (i.e. "Big Data") in view of improving performance or to implement quantitative and rules-based approaches to investing (e.g. "strategic beta"); and

(iv) Standardising existing reporting requirements (i.e. "RegTech").

Presently, these applications are still largely untested, as legacy systems will gradually be replaced to support a new product offering, or new means of service delivery to clients. Much unlike a general

[1] Within this category, we note that applications may differ considerably; ranging from reference data management in the authentication of data regarding funds, to the trading, clearing and settlement of financial instruments (e.g. OTC-derivatives); from fund order processing, (e.g. the joint "Funds Harbour" project in Portugal, in partnership with Deloitte and the Portuguese Asset Management and Pension Funds Association, APFIPP), to the on-boarding of customers via KYC/AML-assessments.

rue Montoyer 47, B-1000 Bruxelles
☎ +32 2 513 39 69 • Fax +32 2 513 26 43 • e-mail : info@efama.org • www.efama.org • VAT Nr BE 0446.651.445

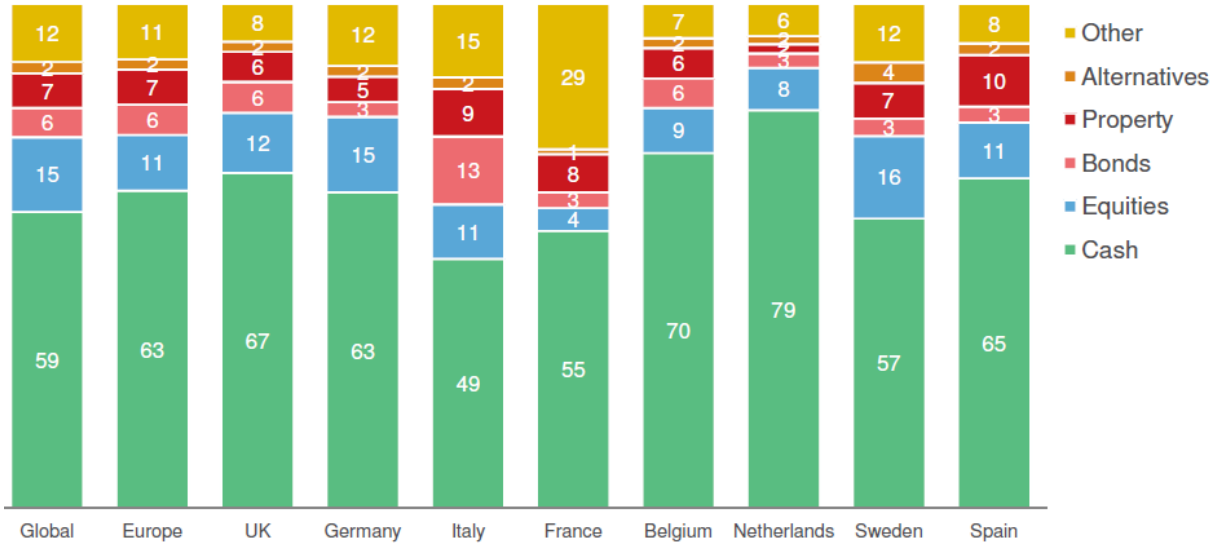
public perception around their "disruptive" nature, these innovations will not systematically entail changes to existing national legislation emanating in turn from EU law.

The gradual take-up of these applications by the European "buy-side" industry will also depend on other service providers working closely with asset management firms, e.g. custodians, accountants, transfer agents, distributors, etc.

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.

Although data on the number of consumers making use of automated advice services remains difficult to obtain at this early stage of development, research from one of our global Members suggests there is a considerable potential for demand, as a large proportion of individuals still choose to hold onto their savings in cash, rather than in investment options, whether these be equities, bonds, alternative assets, etc. By holding an excess of their savings in cash – especially in low interest rate environments – individuals are faced with very poor long-term returns, further weakening their future spending power. The Chart I below crystallises this state of affairs, drawing from the results of a global survey conducted by one of our global asset manager members.

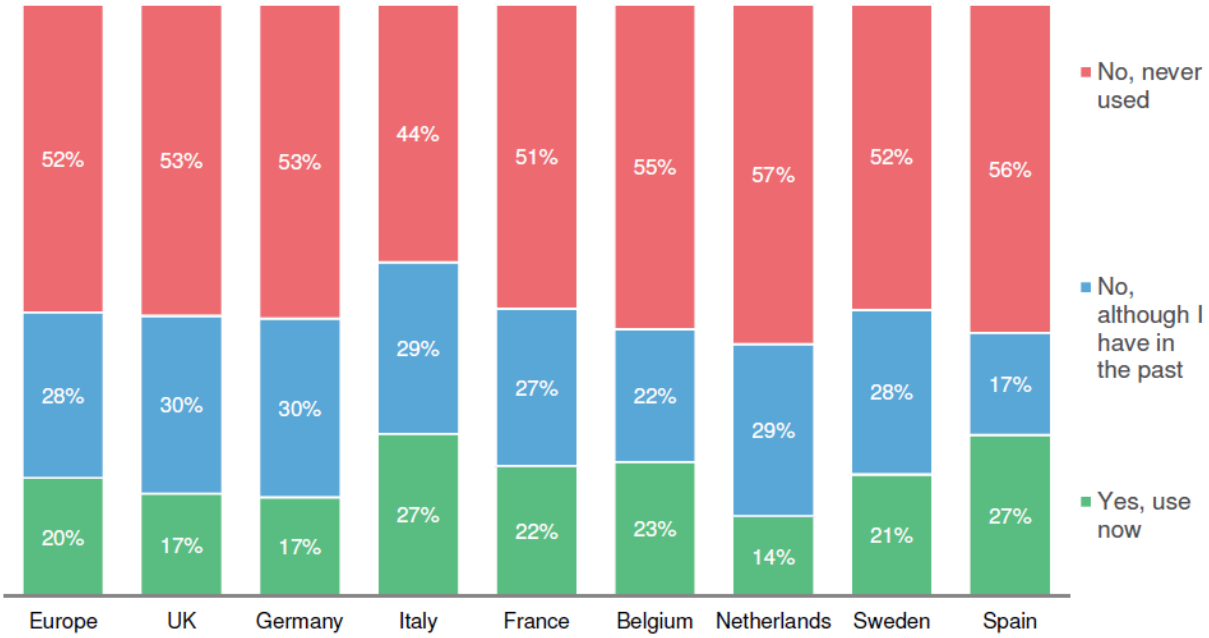
Chart I – Asset Allocation as % of overall Portfolio, per country



Source: Blackrock Investor Pulse Survey 2015

At the same time, average life expectancy has increased significantly since most retirement systems were established and numerous studies project that consumers' retirement contributions will not be adequate to satisfy their financial needs throughout retirement. Compounding these issues are an overall lack of engagement, low financial literacy, as well as insufficient or costly access to advice. Chart II below captures the recent state of affairs across a number of European jurisdictions.

Chart II - Use of Professional Financial Advisors in selected European Countries



Source: Blackrock Investor Pulse Survey 2015

Given the need for European consumers to invest more of their savings, automated financial advice could, especially for the more "tech-savvy" consumers, be of benefit. Access to automated advice services would allow technology to "bridge the gap" with currently untapped groups of investors. Given the current low interest rate environment, coupled with the need for individuals to increase their allocations to fund their own long-term financial needs, especially in terms of retirement, automated financial advice may encourage investment by new groups of investors, who may not have had previous access to a financial adviser.

Other benefits could include a greater degree of transparency *vis-à-vis* a non-sophisticated investment public through an easy-to-use interface and possibly lower fees due to the highly automated nature of the service. As an asset allocation tool, reliance on algorithms promises to optimize an individual's asset allocation based on his/her preferences, risk tolerance, investment horizon, savings rate, tax situation, etc., all while potentially contributing to investor protection by increasing the precision of the information received, increasing the understanding of fund products, as well as of the investment process, thereby also improving the degree of financial literacy for a larger target audience.

Looking more closely at the types of automated advice, these would fall under two broad categories: (i) systems offering fully-automated, end-to-end execution-only services to clients with no human interaction; and (ii) others operating as "hybrids" by presenting investors with a suite of suitable investment portfolio solutions through automation, while still entrusting the final investment advice to a human advisor. Compared to a fully-automated system, which may limit its offers to client profiling, a suitability test and a range of allocation proposals, a "hybrid" solution may better account for changes in an individual's financial profile (e.g. a new income situation, the inheritance of private wealth, a change in tax or family status, etc.) throughout his/her life. There would therefore be a continued need for companies offering automated services to maintain a variety of "access points" to their clients, while allowing the latter to verify the investment process and evolutions of a product's life on an ongoing basis. Also reinforcing the resilience of the human element is the fact that even for

fully-automated platforms, the human advisor will possibly need to be accessible online, via chats or video-calls to explain the investment process in more detail or answer eventual investor queries. We conclude that automated advice will not substitute human interaction, as an advisor may need to respond directly to specific questions and provide information the consumer requires more adequately. A human advisor may also gain a deeper understanding of the financial literacy of the client and may provide answers where a standardised and automated advice is not suitable.

From a definition perspective, it is important to point out that there seem to be different notions of "advice", depending also on which types of products (e.g. mortgage, insurance, investment, pension, etc.) are intended. Particularly in the EU, different types of advice are regulated differently and have different scopes depending on whether they fall into the banking, insurance or securities (investment management) remit. Even within such categories, there are important differences to be made. Generally, in a more global context, the term "advice" will need to be broad enough to encompass all or most of an individual's financial needs.

A barrier to the uptake of automated advice is represented by the need for providers to aggregate client data to achieve a reliable degree of visibility over an individual's assets and liabilities. Such details are typically not all held in one place, obliging the individual to grant access to data stored at third-parties (e.g. banks, insurers, pension funds, tax authorities, to name only a few). As trustworthiness, especially in terms of data protection, will be key for FinTech companies, it is of the utmost importance that all market participants adhere strictly to current rules relating to the use and protection of consumer data.

1.3. Is enhanced oversight of the use of artificial intelligence (and its underpinning algorithmic infrastructure) required? For instance, should a system of initial and ongoing review of the technological architecture, including transparency and reliability of the algorithms, be put in place? What could be effective alternatives to such a system?

Automated investment advice should – on par with traditional (human) advice – be discharged on the basis of a license issued by a national market supervisor and following a thorough assessment of the advice provider. As with any model or algorithm, oversight, in the form of a robust framework for documentation, development, testing and maintenance of systems, should be in place to ensure the chosen technology delivers a consistent outcome based on the information provided by the consumer. In view of this, supervisors should seek to develop competences to ensure that appropriate knowledge and experience exists for providers to offer such automated services and procedures in place for them to oversee the performance of their applications (e.g. algorithms) on an ongoing basis.

As one specific aspect of providing investment advice via automated platforms, such systems should also be programmed in a way that takes into account the fact that consumers may not always provide their information in a consistent way. In order to provide a consistent output, the systems have to be able to deal with inconsistencies of the input. Consequently, the service provider should have the capability to review its automated systems, initially and on an ongoing basis, as a necessary condition for it to continue benefitting from its license.

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)?

It is difficult to define minimum characteristics and the amount of information in general terms. This very much depends on the set-up of the automated advice function. The automated adviser should ensure that investment professionals with sufficient expertise are closely involved in the development and ongoing oversight of the algorithms. As a general rule of thumb, the algorithm's assumptions should be based on generally accepted investment theories that take into account the historic returns of different assets.

More generally, by virtue of the fact that regulation should strive to be technology-neutral, information about the service user should be no different from those information requirements presently laid out in existing regulation (in terms of AML and KYC requirements for instance, as well as in terms of saving habits, personal income, tax status, etc.).

1.5. What consumer protection challenges/risks have you identified with regard to artificial intelligence and big data analytics (e.g. robo-advice)? What measures, do you think, should be taken to address these risks/challenges?

Generally speaking, challenges relate to the success of new means through which to access clients and the most comprehensive, cost-efficient and safe way to make use of their related personal information. Looking more specifically at robo-advice, we would suggest the following two high-level principles to underpin future policy-making:

a) Clients should understand what services they are receiving and the potential risks involved; and

b) Digital advisors should disclose the costs clients can incur (including fees), in line with the existing transparency requirements.

From a regulatory perspective, it is important to recognise that digital advisors should broadly be subject to the same framework of regulation and supervision as traditional advisors, although the applicability and emphasis of existing regulations may differ in some cases. Worth considering are a number of key areas:

1. Know your client and their suitability requirements: Like traditional advisors, digital advisors must make suitable investment recommendations based on their knowledge of clients' circumstances and objectives. Whether or not this information is obtained through an online questionnaire or more traditional means, it should be used to make appropriate recommendations based on the clients' goals. Important that MiFID suitability guidelines recognise the digital take on procedure;

2. Algorithm design and oversight: A key component of digital advisors' service models is the use of optimisation algorithms. Digital advisors should ensure that investment professionals with sufficient expertise are closely involved in the development and ongoing oversight of algorithms. Algorithm assumptions should be based on generally accepted investment theories that take into account the historic returns of different asset classes, and key assumptions of the algorithms should be made available to investors;

3. Disclosure standards and cost transparency: Clients should understand what services they are receiving and the potential risks involved. Digital advisors should clearly disclose the costs clients can incur (including fees), as well as other forms of compensation. In addition,

advisors should disclose relevant technological, operational, and market risks to clients. This should include information on the tools the advisor can use to address these risks and when they would use such tools;

4. Trading practices: Like traditional advisors, digital advisors generally manage client assets on a discretionary basis and buy or sell equity securities, ETFs, and other broad-based securities. As part of these services, digital advisors should have reasonably designed trading procedures that include controls to mitigate risks associated with trading and order handling. Trading and portfolio management capabilities should be supervised by skilled investment professionals;

5. Data protection and cybersecurity: Digital advisors should view cybersecurity as a critical component of their business model and carefully safeguard sensitive client information. Digital advisors should use the strongest data encryption, conduct risk management of third party vendors, obtain appropriate levels of cybersecurity insurance, maintain business continuity management plans, and implement incident management frameworks.

In this age of technology, we should expect an ongoing evolution of the digital advice landscape. As business models continue to evolve, it is important that regulatory regimes encourage innovations that could be beneficial to consumers.

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

EFAMA has no comments in this regard.

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?

Regardless of the nature and format of non-bank financing solutions available through the use of FinTech, any support from public authorities should guarantee an equivalent level of protection to investors, especially in terms of the quality and accuracy of the information that they receive.

1.8. What minimum level of transparency should be imposed on fund-raisers and platforms? Are self-regulatory initiatives (as promoted by some industry associations and individual platforms) sufficient?

We believe that fund-raisers and platforms which offer regulated services should be subject to the same regulation as any other players in the market, especially in terms of transparency.

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?

EFAMA has no comments in this regard.

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.)?

EFAMA has no comments in this regard.

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?

Beside the elements raised in our response to Question 1.1 above, we see no additional technologies that would be particularly innovative.

Section II - Bringing down operational costs and increasing efficiency for the industry

2.1. What are the most promising use cases of FinTech to reduce costs and improve processes at your company? Does this involve collaboration with other market players?

At this stage of development for numerous initiatives yet to be finalised, EFAMA sees the first benefits in the reporting space (i.e. reporting contracts or reporting transactions).

A second level of development that could help reduce costs is the use of "Big Data" features to help develop reporting architectures and actual reports[2].

A third level of development could come from the collection and treatment of a wide range of information of companies open to external investment. These data could enhance strategic investment decisions. However, a practical issue resides in the current insufficient standardisation of data which must be addressed first.

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?

In general, EFAMA would caution the European Commission against taking a too proactive stance when most of the technology and its applications are still being developed and experimented with. Although a number of EU jurisdictions are experimenting with the regulatory "sand-box" approaches, we observe that the few and more promising FinTech applications in our industry are still far from assuming a clear "EU dimension". Rather, we would advocate for measures to be taken at the EU level only once such applications "find their ground".

[2] With regard to the definition for "Big Data", we refer to the definitions used by the EU Commission on its website; available at: https://ec.europa.eu/digital-single-market/en/big-data

With regard to distributed ledger technology (DLT), national initiatives remain worthwhile, although in view of their application in the broader EU and global markets, some form of EU level coordination would be helpful, particularly in light of revised MiFID rules on transparency and on the definition of venues. Although firms may deem the legislative scope offered by MiFID to allow for new forms of business, firms also foresee difficulties were they to "test run" their DLT-related projects, given that forbearance does not exist in EU law. Coordination among national competent authorities with input from ESMA (in turn supported by the European Commission) would create a favourable environment for those DLT projects needing a larger testing space. For instance, one could imagine the challenge to develop a DLT for custody chains under the current framework offered by the UK FCA, where the transaction of a GBP denominated instrument is between a UK seller and a German buyer, albeit where the custodian is a French provider and the fund accountant a German entity.

The questions of interoperability of DLTs and their integration in existing harmonised markets will also require dedicated coordination at least through ECB T2S workstreams.

Furthermore, the European Commission should also continue to support the Member States' efforts to advance electronic identification and trust services for electronic transaction in the internal market (e-IDAS) in order to accelerate the cross-border and cross-sector use of electronic identification (e-ID), including mobile ID and trust services for digitally enabled businesses. We believe that an increased usage of e-IDs will also allow an easier up-take of FinTech solutions around Europe.

Last but not least, the European Commission may also have a closer look at the existing ISO efforts which are mapping the existing standards around FinTech in the EU. We greatly endorse the current ongoing mapping exercises and believe that such standards are desirable to create the right environment for any type of FinTech solution.

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?

As with past technological breakthroughs, the impact of increased automation in the financial services industry may impact employment, and specifically, for those functions previously entrusted to people. As a result, one part of the workforce may be reassigned or encouraged to develop new skills in the process. Retraining is perhaps the best way to help those disrupted by advancements in technology and ensure that automation of repetitive activity, which would otherwise be performed manually, allows for the workforce to be positioned around higher-value tasks and functions.

2.4. What are the most promising use cases of technologies for compliance purposes (RegTech)? What are the challenges and what (if any) are the measures that could be taken at EU level to facilitate their development and implementation?

With an increased emphasis in meeting regulatory requirements, compliance has important operational impacts on investment management companies, beckoning the need for new reporting solutions. In this context, FinTech providers may be of valuable aid in helping these companies tackle their data and reporting challenges, thus leading to the emergence of the related concept of "RegTech".

According to a recent report, published jointly by the Association of the Luxembourg Fund Industry (ALFI) and Deloitte[3], the RegTech proposition would mostly relieve a company's heavily quant-based and information-based obligations, including risk identification and management tools, legislation/regulation gap analysis, compliance, information management, transaction and regulatory reporting to name a few. Over the nearer term, RegTech may help investment management firms to automate the more work-intensive compliance tasks and reduce operational risk and costs associated with meeting compliance and reporting obligations. Over the longer term, RegTech promises to empower compliance functions to better assess the compliance risks that they face and how they mitigate and manage those risks. Compliance officers will therefore require technological support to anticipate regulatory change, identify impacts, monitor regulatory readiness, and perform ongoing controls. A comparable use may eventually also be taken-up by national securities regulators in automating and aggregating reported data in view of carrying out their supervisory and/or policy-setting mandates.

As a precondition for RegTech to deliver its future potential, it is key for the Commission to develop harmonised standards of reporting, especially for financial instruments (e.g. through the use of ISIN codes, including for OTC Derivatives). Important in this respect is that the Commission continue its efforts to streamline regulatory reporting away from unnecessary duplications.

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

EFAMA has no comments in this regard.

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

EFAMA has no comments in this regard.

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

In the short term, we do not consider use of DLT as a relevant mean to help financing SMEs, nor the larger economy, although this may change over time through the development of certain use cases. The most immediate benefit of DLT is the improvement of legal certainty. A second-order benefit would be some efficiency gains from the disintermediation of some service providers in term of cost reduction. To the extent DLTs are not publicly mandated, there may also be disadvantages on the basis of their restrictive access.

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

[3] Please refer to the joint report "How can Fintech facilitate fund distribution?", published on 4 March 2016; available at: http://www.alfi.lu/sites/alfi.lu/files/files/Publications_Statements/Surveys/How-can-fintech-facilitate-fund-distribution-final.pdf

All points raised in the above question are indeed part of the constraints tied to the use of DLT. An element of data standardisation that is of key importance is the format of the data and use of existing communication standards to the largest possible extent (e.g. ISO 15022 or ISO 20022).

Another major challenge is to provide for a regime that facilitates the confirmation of transactions. Under existing reporting regimes, the number of fields that are requested to be reported without errors frequently causes reports to be rejected. Focusing on key data formats (i.e. LEIs, UTIs, UPIs, ISINs and prices as a minimum) could facilitate the automation of reporting, consequently fostering the development of DLTs.

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

At this early stage and considering the limited use of DLT outside ongoing pilot-projects, we do not have sufficient information to indicate any regulatory or supervisory obstacles. As the Commission considers a regulatory approach to DLT, we would note the following:

- DLT is at an early stage of development and deployment. Therefore, it is important that any regulatory approach to DLT does not implicitly limit or constrain firms' ability to test and develop DLT solutions;
- The potential uses for DLT are numerous and diverse. Any regulatory framework needs to be sufficiently cognizant of the diverse potential applications of DLT that are adaptable to operating across multiple activities and services. Consequently, the adoption of a "one size fits all" regulatory framework for DLT is unlikely to be effective;
- If a situation arises where the use of DLT poses challenges within a certain regulation, policymakers should take a pragmatic approach to such situations; and
- Harmonised international approach – In order to provide an effective regulatory framework which is facilitative, this framework should be based on harmonised international standards rather than on local regional requirements. Divergent regulatory approaches to DLT would likely hinder DLT's deployment in practice.

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

EFAMA has no comments in this regard.

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.

In general, with a view to outsourcing requirements, the entity offering investment advice directly to the client should bear the ultimate responsibility before the latter. Outsourcing agreements with external, third-party providers which may provide the entity with the underlying technological applications, IT support infrastructure, algorithms, etc. should by no means imply less liability for the

direct provider of the service. As a result, such providers should choose third parties on the basis of a documented and thorough due diligence process, while exercising an ongoing review of their performance and offering adequate escalation procedures in the event problems are encountered at the level of the third-party.

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?

With regard to the application of DLT, one obvious solution would be the creation of a DLT for the reconciliation and reporting purposes of buyers and sellers of OTC-traded instruments. The bespoke nature of those contracts needs tailored contracts, often documented by master agreements. These agreements require lengthy negotiations before execution and would benefit from having one location for follow-up negotiations within a certain date of execution.

Another possible solution which needs to be examined is the creation of a DLT for taxation purposes, especially in the area of withholding taxes. Claiming WHT (withholding tax) relief under Double Taxation Agreements and/or a country's domestic tax laws is often cumbersome and time and resource intensive for governments, financial institutions, and foreign portfolio investors. The European Commission already noted in the past that a withholding tax relief procedure at source, rather than through a refund procedure, would facilitate the situation. A tax relief at source procedure is, however, only possible if the party that is responsible for withholding the tax amount has the necessary information about the investor when the transaction takes place. In a lot of cases this condition cannot be fulfilled. A DLT could eliminate the imbalance of information among market participants and therefore support withholding tax relief procedures at source.

Section III - Making the single market more competitive by lowering barriers to entry

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?

With regards to automated advice, it is important to recognise that digital advisors are subject to the same framework of regulation and supervision as traditional advisors, although the application and emphasis of existing regulations may differ in some cases. In these cases, regulators could consider the currently existing paper-based disclosure requirements (i.e. a three-page PRIIPs KID) and assess how such disclosures could be meaningfully transposed to the new "screen-based" environment.

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

The active involvement of national supervisors has proven critical in helping innovative start-ups, as well as applications from market incumbents, find the comfort of a responsive environment where FinTech solutions can be tested against existing regulatory requirements. The exchange has proven mutually beneficial, for private sector actors becoming accustomed with existing regulations

(especially in terms of investor protection), as well as for the official sector to appreciate the breadth and innovative potential of numerous solutions offered by private enterprises. EFAMA deems that such degree of mutual cooperation should be allowed to ripen further at the national level, possibly leading to closer cooperation between authorities once certain businesses with their proposed services achieve a critical size to begin marketing cross-border. We insist that the latters' success be determined by end-consumers and investors collectively, away from any pan-European initiative at least at this early stage.

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.

At this early stage and due to the general lack of existing "live" projects or offerings, we consider that presently there is no regulatory barrier that would need to be addressed. We note that the Commission, as stated in its CMU Mid-Term Review, will assess the case for an EU licencing and passporting framework for FinTech activities in Q4 2017.

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?

Please refer to our answer to Question 2.2 above. We would caution the EU from taking a too proactive stance at this early stage of development. Furthermore, an EU FinTech licence could create an un-level playing field to other ways of providing services. As above, we note that the Commission, as stated in its CMU Mid-Term Review, will assess the case for an EU licencing and passporting framework for FinTech activities in Q4 2017.

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.

Generally, enhancing the coherence of the EU regulatory framework is positive per se, as it materially improves its practical application, allows efficiency gains for market participants and facilitates effective supervision.

Regarding the principle of proportionality, we would caution against its application leading to a "lighter" regulatory regime for certain providers compared to that for established market incumbents. In other terms, the principle of proportionality should not trump the other founding principles underpinning the Commission's proposed framework for FinTech, i.e. the principle of technological neutrality and that of integrity.

3.6. Are there issues specific to the needs of financial services to be taken into account when implementing free flow of data in the Digital Single Market? To what extent regulations on data

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

EFAMA has no comments in this regard.

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

Yes, we believe so. These principles, however, should not only apply to the FinTech activities. More broadly, they should continue to inspire sound policy making in financial services.

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?

Please refer to our answer to Question 2.2 above.

We would caution the EU from taking a too proactive stance at this early stage of development, be it through more tangible initiatives from the Commission or via the ESAs. We believe instead that the market, guided by consumer choice and preferences, should firstly and more concretely better define service needs and select the most promising providers on this basis. Exchanges with several of the European national supervisors have demonstrated that the bulk of FinTech enterprises offer services that can be regulated under existing (EU) provisions, while allowing for the most promising applications to build sufficient scale. With a view to increasing supervisor expertise, we encourage coordination at an EU level, be it through joint working group sessions or other means, but note that it also remains important for FinTech companies to maintain an exclusive relationship with their domestic regulator by virtue of its proximity and knowledge of the local rules regulating the business environment. There are risks that any overly-burdensome, EU-wide initiative would allocate resources less efficiently, while being less sensitive and responsive to local market realities at this early stage.

Notwithstanding the above, for the reasons illustrated in our answer to Question 2.2 above, coordination between the European Commission and the ESAs (especially between ESMA and EBA from their respective market and credit oversight perspectives) to foster the cross-border development of DLT initiatives, as well as those for more cross-border and cross-sector use of forms of electronic identification (e-ID), remain desirable.

Furthermore, in a more general sense, EU and global harmonisation of standards will eventually be key to realising the full benefits of FinTech. FinTech firms have the ability to operate across jurisdictions, as their new technologies being developed are not limited by geographic boundaries or a single legal and regulatory regime. As global regulatory bodies (FSB/IOSCO/Basel/ECB Eurosystem T2S) continue to monitor this space, they should help coordinate FinTech-focused policies from member jurisdictions within the EU.

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?

EFAMA would welcome the approach of an "Innovation Academy", which could mirror a similar approach used for the European Post-Trade Forum (EPTF), bearing a strategic committee, seconded by three expert groups on, for instance, (i) investor protection (for the automated advice-related services); (ii) market activities (for DLTs, smart contracts, algorithms, etc.) and (iii) cyber security.

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?

Please refer to our answers to Questions 2.2 and 3.8 above.

We believe that it is important for national competent authorities to support start-up companies – including FinTechs - while becoming familiar with various types of technology, developing their IT literacy and skill-sets. In this regard, close exchanges with FinTech start-ups remain extremely precious for educational purposes, benefitting private-sector entrepreneurs as well, especially those approaching the regulator for the first time and keen to be regulated in order to build trust and establish their brand. Only subsequently, as a second stage development and only once certain applications have been vetted by the market and achieve sufficient scale, could initiatives at the European level lay out principled foundations for partnerships between two or more jurisdictions, or in view of an EU-wide licence to passport services.

Exceptionally, with regard to the development of DLT, we believe there should be some degree of coordination between competent authorities/ESMA from the beginning of a given project, in order to avoid duplication of efforts and possible spill-over effects were pilot-projects to not be successful.

Furthermore, in a more general sense, EU and global harmonisation of standards will eventually be key to realising the full benefits of FinTech. FinTech firms have the ability to operate across jurisdictions, as their new technologies being developed are not limited by geographic boundaries or a single legal and regulatory regime. As global regulatory bodies (FSB/IOSCO/Basel/ECB Eurosystem T2S) continue to monitor this space, they should help coordinate FinTech-focused policies from member jurisdictions within the EU.

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.

We would see benefits in extending the monitoring and development of guidelines to every aspect of innovation, therefore also ensuring the compliance of portable applications (such as "apps") in line with the existing legal framework.

Additionally, considering the high volumes of data to be maintained and exchanged, as well as the international nature of the transactions and clients subject to the reporting requirements, we would see merits in creating a "data roaming" regime, especially from a "Big Data and" RegTech perspective. Without such a regime for the international alignment of data transfer costs, we fear that data providers could increase data transfer costs when regulatory compliance requirements will be streamlined through DLTs.

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?

EFAMA has no comments in this regard.

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

Please refer to our answers to Questions 2.2 and 3.8 above.

The potential for FinTech applications should firstly be scoped locally. Once successful, a technological application will inevitably be proposed or taken-up elsewhere, at which point, while not necessarily requiring the active intervention of regional or global policy makers, the success of implementation across jurisdictions will depend on a harmonised international approach. For instance, once the take-up of DLT becomes more decisive within sell-side institutions, given that these often have a significant cross-border presence and transact with numerous other counterparts (*inter alia* buy-side institutions), naturally these other players will have a natural incentive to adopt the same technology in view of becoming more interoperable. In this respect, we deem the recent findings of the ESMA final *Report on the Distributed Ledger Technology Applied to Securities Markets*[4] of 7 February 2017 to be sensible when concluding that "(…) it is premature to fully appreciate the changes that the technology may introduce and that any regulatory action would be precipitate".

As legal questions will arise while technology develops and its applications become more visible, we consider it is presently too early to call for EU-wide standard-setting. The latter would inevitably introduce greater fragmentation in an already overly complexed regulatory environment, where proper definitions may still be lacking (e.g. as the notion of "investment advice", or that of "marketing"). Preferably, it is only once the success of certain FinTech applications becomes clearer, that a closer dialogue between market participants and EU policy-makers and regulators should occur in view of establishing cross-border frameworks.

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?

Open-source architecture may be useful to:

- Reduce implementation costs;
- Facilitate portability and access; and
- Avoid entry barriers.

[4] Please refer to the ESMA final Report (ESMA50-1121423017-285); available at: https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf

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.

We have no specific comments with regard to the impacts on incumbent firms.

With regard to the efficiencies market incumbents would stand to gain from use of FinTech applications these may vary widely. For our industry, we note that the use of automated advice, for instance, promises to enlarge product distribution networks and reach new clients, while at the same time offering human advisors a better overview of client preferences, ideally over a longer-term life-cycle horizon, in view of better tailoring investment advice. The growing use of artificial intelligence would for instance allow incumbents to therefore harness the ever-growing diversity of investor information in the form of separate data points in view of providing better client profiling, ahead of tailoring a more suitable investment product.

The opportunity to exploit artificial intelligence has also prompted large incumbents with sufficient means to invest heavily in electronic data mining capabilities, capturing actionable intelligence from various sources (e.g. from social media, blog platforms or market information from financial media) with the aim of successively integrating it into their investment process. In this sense, such capabilities are able to provide additional data points and signals on which to trade on behalf of clients, thus allowing firms to achieve an "edge" over their industry competitors.

On their part, market incumbents are proving critical as business partners for smaller FinTech companies or start-ups, by committing the initial funding, knowledge, data, office space, which are critical to achieving a critical scale.

Section IV - Balancing greater data sharing and transparency with data security and protection needs

4.1. How important is the free flow of data for the development of a Digital Single Market in financial services? Should service users (i.e. consumers and businesses generating the data) be entitled to fair compensation when their data is processed by service providers for commercial purposes that go beyond their direct relationship?

The importance of the free flow of data may be best illustrated by the use certain portfolio managers make of "Big Data", through the analysis of available market and company data and financial market trends for their portfolios, across several investment strategies. Unrestricted access to market data leads to better and more informed decisions, more efficient processes, and more appropriate services for the end clients. There is an increase in data firms can collect from the market place, as well as from their own sales operations to generate consumer-led market insights. Therefore, an open access to all data sources for portfolio managers without restrictions is a prerequisite.

In general, current and forthcoming data protection legislation provides consumers with adequate protections and greater transparency into how their data is used and ability to consent and opt-out, and also ensures that service providers do not process data for purposes that go beyond the purposes for which the data were collected. This provides appropriate protection, limiting the need for a system of compensation in return for data use.

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

Should the data required be standardised, DLT would provide a reliable and stable source of transactions' information. It is our understanding that the use of commercial initiatives to develop DLT seems to be a preferred option by the EU Commission. From our perspective, this could cause some issues, especially in terms of fragmentation and access to data for price formation purpose, especially under MiFID II / MiFIR reporting requirements.

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

The use of identifiers must be favoured at all level of reporting, for every type of requirement (i.e. LEIs, UTIs, UPIs, and ISINs) and by the use of standardised messaging (ISO standards).

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

From our perspective, the proposed regime should distinguish between two situations:

(i) The first situation is the relationship at the level of the individual (personal) advice. In the related circumstances, the current rules on personal data protection[5] that entered into force in May 2016 must apply; and

(ii) The second situation is where an individual is part of larger system, in which case, we would recommend to use the definition and the regime set in the Directive on settlement finality in payment and securities settlement systems[6] and to set the identification at the level of the funds (or sub-funds), rather than at that of the individual client.

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?

EFAMA has no comments in this regard.

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?

EFAMA has no comments in this regard.

[5] The EU Regulation (2016/679) and the Directive (2016/680) on data protection of 27 April 2016 have been published in the EU Official Journal the following 4 May. While the Regulation has entered into force on 24 May 2016, it shall apply as from 25 May 2018. The Directive has entered into force on 5 May 2016, for EU Member States to transpose it into their national law by 6 May 2018.

[6] Please refer to Directive 98/26/EC on settlement finality in payment and securities settlement systems; available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01998L0026-20140917

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?

As an Affiliate Member of IOSCO, EFAMA has contributed significantly to the work of the global standard-setter in the realm of cybersecurity over the past couple of years. As the European buy-side association and jointly with other non-EU buy-side organisations, we have developed a survey tailored to the specificities of the asset management sector. We have administered the survey twice over the past two years and results were positive.

In terms of minimum requirements for each firm, we have identified the following best practices:

- Identification of the firm's key digital assets (including intellectual property, critical business processes, shareholder information and other confidential data, and key operating facilities) to allocate resources where the risks may be higher for the firm; firms should develop a clear understanding of normal network functions, activity, and links;
- Implementing effective control and protection measures, involving, among other tools, username and password protection, control of administrative and privileged access, removal of "undesirable" applications, anti-virus protection, mobile device security, and encryption of data;
- Implementing ongoing training for employees (including legal staff) and develop an effective security culture of responsibility and accountability throughout the firm;
- Ensuring an appropriate monitoring of system and data usage to facilitate the identification of abnormal patterns;
- Developing detailed and actionable incident response plan, with clear roles and responsibilities, communication procedures and possible remediation measures; when an incident does occur, firms should be prepared to document their actions;
- Accessing and sharing actionable threat information, as well as building peer network to share expertise, experiences and increase "circles of trust" that include law enforcement;
- Engaging with third parties to conduct due diligence reviews of a service providers' information security program, and understand if fourth party service providers are utilised; and
- Ensuring an ongoing reassessment of the firm's cyber resilience, its vulnerabilities, and protection, including by benchmarking against industry practices and peers.

Proportionality must be guaranteed as asset managers operate their own business model that remains distinctly different from that of other market players. Harmonisation efforts, if at all, should therefore remain principle-based. Already, domestic regulators are starting to promote a robust cyber-security posture across the industry through guidance. It is broadly acknowledged that a detailed and prescriptive "one-size-fits-all" approach to regulating cyber risks will not work, given the pace of technological innovation, the changing sophistication of adversaries and the ever-growing expansion of the threat landscape.

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

Data protection legislation is often cited as being the main impediment to closer cooperation with public enforcement authorities. Such data would not only relate to individual clients/customers, but could also concern very sensitive business data whose leakage could seriously affect the viability of a firm's business. Having said this, it should be noted that firms often collaborate with other members of the financial industry beyond interaction with governments and regulators. The belief that cybersecurity is not a competitive issue has allowed the industry to work together to improve the cyber defences of the sector as a whole. Information sharing and coordinated analytic work have been the hallmarks of sector collaboration.

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

As part of global problem, cybersecurity deserves a coordinated response at the broadest level possible around risk-based approaches to cybersecurity risk management. Regulators around the globe have taken varying approaches to cybersecurity concerns. Some have focussed on specific management arrangements to address cyber-threats (e.g. policies, procedures, etc.); whereas others have opted for a more principle-based approach, whereby cybersecurity is covered by the broader conduct obligations/operational risk management arrangements. In addition to clarifying their expectations with regard to how firms approach cybersecurity, regulators have started conducting specific examinations and an increasing number of investment managers stands to be sanctioned for failings in their cybersecurity practices.

However, any rules on a supranational level also need to address enforcement issues.

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?

EFAMA has no comments in this regard.

***

Brussels, 15 June 2017

[17-4024]