MANAGED FUNDS ASSOCIATION
The Voice of the Global Alternative Investment Industry
WASHINGTON, DC | NEW YORK

June 15, 2017

Via Electronic Submission

DG Financial Stability, Financial Services and Capital Markets Union
European Commission
SPA2 02/076
1049 Brussels
Belgium

Dear Sir or Madam,

Re: Fintech: A more competitive and innovative European financial sector

Managed Funds Association ("MFA")[1] welcomes the opportunity to provide comments to the European Commission (the "Commission") on its consultation document "Fintech: A more competitive and innovative European financial sector" (the "Consultation Paper"). MFA members, as investors in European markets and professional asset managers for European institutional investors, have a shared interest with the Commission and other EU legislators in the development of an appropriate policy framework for FinTech in the EU. MFA therefore supports the Commission's efforts to promote competition, innovation and risk management in this area.

We have focused our response to the Consultation Paper on issues relating to automated advice and execution, distributed ledger technology ("DLT"), RegTech (particularly in relation to regulatory reporting) and cyber security. We have submitted responses to specific questions using the Commission's online form. These are also set out below for your ease of reference.

MFA would like to reiterate its thanks to the Commission for the opportunity to engage constructively in these issues. We would welcome the opportunity to discuss our views in greater

[1] Managed Funds Association ("MFA") represents the global alternative investment industry and its investors by advocating for sound industry practices and public policies that foster efficient, transparent, and fair capital markets. MFA, based in Washington, DC, is an advocacy, education, and communications organization established to enable hedge fund and managed futures firms in the alternative investment industry to participate in public policy discourse, share best practices and learn from peers, and communicate the industry's contributions to the global economy. MFA members help pension plans, university endowments, charitable organizations, qualified individuals and other institutional investors to diversify their investments, manage risk, and generate attractive returns. MFA has cultivated a global membership and actively engages with regulators and policy makers in Asia, Europe, North and South America, and many other regions where MFA members are market participants.

detail. Please do not hesitate to contact Jennifer Han or the undersigned at +1 (202) 730-2600 with any questions that the Commission or its staff may have regarding this letter.

Respectfully submitted,

/s/ Stuart J. Kaswell
Stuart J. Kaswell
Executive Vice President & Managing Director,
General Counsel
Managed Funds Association

/s/ Michael Pedroni
Michael Pedroni
Vice President, International Affairs
Managed Funds Association

MANAGED FUNDS ASSOCIATION

RESPONSES TO QUESTIONS IN THE CONSULTATION ON FINTECH

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

MFA members use FinTech applications for a range of purposes, including automated trading strategies, clearing and settlement of trading in financial instruments, posting of margin and collateral, smart contracts and trading confirmations, monitoring for regulatory and market abuse purposes, as well as for regulatory and investor reporting processes. Such FinTech applications enable asset managers to tailor their services to the needs of their investors and to increase the speed, quality and efficiency of trading and reporting processes. This helps to reduce costs for asset managers and investors and to improve market standards of trading and portfolio management activities and reporting processes.

MFA hopes that FinTech solutions in these areas will continue to develop and to be employed by market participants for the benefit of investors and the functioning of financial markets generally. The success of such FinTech solutions in the EU will depend on flexible, technologically neutral, principle-based regulation of areas such as automated trading strategies, post-trade processing and reporting, DLT and cyber security. It will also require that regulators make investments in their systems to keep pace with technological change and improve efficiency and accuracy of regulatory reporting solutions and in their own cyber security. Such developments would encourage growth and innovation as well as greater cooperation between market participants and regulators in protecting financial markets from common threats such as theft of intellectual property and cyber attacks.

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.

Our members are not primarily in the business of providing advice to retail investors, automated or otherwise. However, technology and algorithms enable asset managers to tailor their services to the needs of particular investment funds and institutional investors. For example, portfolio construction services give asset managers the ability to assess a large institutional investor's overall holdings and to tailor investment strategies and portfolio allocation methodologies according to that investor's needs. For example, one investor may have unique social goals that lead it to wish to avoid investing in certain industries. Automation enables firms to adapt portfolios to those investors' needs.

In this regard, MFA notes that there are significant differences between the types of services that are suitable for professional investors and those that might be suitable for retail investors. Professional investors, such as institutional investors and investors familiar with trading in financial instruments are in a better position to assess for themselves what bespoke services they may need from their asset managers. Such professional investors are also more likely to have complex portfolios of investments that require more powerful technological tools to assess and optimise asset management services. In developing principles to regulate "robo advice", for example, the Commission and EU policymakers generally should consider that such a term can encompass a very wide range of activities. It would be unfortunate if regulation of "robo advice" had the unintended

consequence of restricting automated portfolio construction services that asset managers might wish to provide their sophisticated institutional clients, such as insurance companies and endowments.

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

Artificial intelligence (AI) is commonly defined as "intelligence exhibited by machines". In computer science the concept is further refined by reference to an "intelligent agent", which is any device that perceives its environment and takes actions to maximise its chance of success at some goal. The best example of this within the investment field is in trading and execution algorithms which rapidly search across multiple venues to find the best place and method to execute a trade.

The revised Markets in Financial Instruments Directive (2014/65/EU) (the "MiFID II Directive" and, together with Regulation (EU) No 600/2014, "MiFID II") and accompanying regulatory technical standards[2] already address this issue. Article 17 of the MiFID II Directive requires investment firms that engage in algorithmic trading to have in place effective systems, risk controls and business continuity arrangements relating to their trading systems. In particular, such firms are required to have compliance and senior management oversight of their trading systems and to take responsibility for the role of any outsourced service providers in the firm's algorithmic trading activities. Such firms are also required to test algorithmic trading strategies to ensure they do not perform in an unintended manner or lead to disorderly trading conditions.

MFA supports the need for appropriate and proportionate oversight and review of the use of automated trading and execution systems as required under MiFID II. In general, we consider that the MiFID II rules on algorithmic trading, which are intentionally broad, are sufficient to address the current risks posed by the algorithmic trading activities of investment firms. However, in order to achieve robust systemic risk controls pursuant to the MiFID II requirements, it is also important that trading venues, and the brokers that provide other firms with electronic access to them ("direct electronic access"), provide such other firms with appropriate testing environments for algorithmic trading strategies and access to real-time (or near real-time) copies of trade reports and messages related to orders (referred to as "drop copies"). This would enable such firms to monitor and assess their algorithmic trading activities effectively on an ongoing basis.

Policy makers should also exercise care in proposing any extensions to the existing regulatory framework. In particular, it is crucial for market participants that regulatory reporting obligations and oversight measures do not inadvertently undermine security and confidentiality of a firm's proprietary information such as the source code for algorithmic trading and advice strategies. Market participants have a number of legitimate concerns with providing source code to regulators, including:

[2] In particular, *Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organisational requirements of investment firms engaged in algorithmic trading*, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.087.01.0417.01.ENG&toc=OJ:L:2017:087:TOC

- the regulator not being able to maintain the confidentiality of source code information;
- source code could be stolen or misappropriated from the regulator—either electronically or in hard copy; and
- regulators being forced to produce source code in relation to legal proceedings.

In short, the more often that a regulator has possession of a firm's proprietary source code, the greater the likelihood that the information will become compromised, either by hacking or because of the regulator's failure to guard such information carefully.

As a policy matter, regulators should refrain from asking firms to provide them with highly confidential and commercially valuable intellectual property unless this is absolutely necessary and proportionate to an identified risk. We support regulators having the information they need to oversee regulated firms and to monitor markets. However, this authority needs to be balanced against the potential risk of irrevocable harm to the relevant firms and to their clients and investors (e.g. unauthorised disclosure or misappropriation of trade secrets). It is therefore crucial that the legal frameworks under which regulators operate require regulators to exhaust all less invasive means of oversight prior to seeking confidential intellectual property from firms in respect of artificial intelligence and FinTech. Further, where regulators do request such information from firms, it is important that regulators and their service providers are subject to robust confidentiality and data security requirements.

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

Automated trade execution and post-trade processing services are two of the most promising use cases of FinTech in the asset management sector. (See further our response to Question 1.2 above). Please also see our response to Question 2.4 below in relation to RegTech specifically. Many of our member firms use automated analytics to review the vast amount of data available in today's world to make better investment decisions. Many of our members also use sophisticated automated reporting systems to provide secure access to confidential information about their funds to the funds' investors. Use of "cloud computing" solutions for data storage and secure processing systems has reduced the cost of automating critical processes and reporting.

DLT also has significant potential to improve asset management and trading processes through smart contracts and confirmations. Finally we believe that technology and automated systems could be used to improve the speed and efficiency of fund reporting to regulators. See further our response to Question 2.4 (below).

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?

There are three main categories of measures that should be taken to facilitate the development

and implementation of FinTech solutions for the asset management industry:

1. measures to improve governance, data protection and data security standards of exchanges and other trading venues, central counterparties ("CCPs"), and DLT operators;

2. measures to reduce anti-competitive pricing of market and other data; and

3. measures to improve confidentiality and data security standards and resources of national regulatory authorities and the European Supervisory Authorities.

The first set of measures is discussed in our response to Question 2.9 (below). The second and third set of measures are discussed here:

Anti-competitive pricing of market and other data

Data related to the securities and derivatives and other financial instruments in which our members invest is critical to their businesses. They use these data to make investment decisions, to execute trades in the best possible manner for their investors and funds, to manage risks in their portfolios, and to prepare investor and regulatory reports. Data licensing fees are a significant cost for financial services firms, including asset managers. Operators of trading venues and data service providers have a monopoly (or at least an oligopoly) on data, such as pricing and trading volume data, relating to trades executed on certain trading venues. If markets for such data are left unchecked, this gives such operators and service providers the ability to charge significant rents for the use of such data, which is crucial for a broad range of financial services firms.[3]

Such rents result in exaggerated costs for firms and ultimately for their clients and investors. They also discourage firms from using FinTech solutions to improve trading processes, as many such FinTech solutions involve the use of cloud computing or a greater range and volume of trading data and hence higher data fees. Such costs also hinder competition among providers of FinTech solutions and they unduly disadvantage smaller firms and create barriers for new market entrants.

The Commission's efforts as a competition regulator to address such inappropriate pricing and conditions of use by data service providers have helped to mitigate these issues in respect of certain providers. The Commission's action in respect of Standard & Poor's licensing fees for the supply of US International Securities Identification Numbers[4] and Thompson Reuters' licensing arrangements for its Reuters Instrument Codes[5] are clear examples of how proactive supervision of these issues can lead to positive market outcomes. The Commission's decisions in these cases enabled

[3] As regards abuse of a dominant position by data service providers, see for example the judgment of the General Court of the European Union in *Case T-76/14 Morningstar, Inc. v Commission*, available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160100en.pdf

[4] See *Commission Decision of 15.11.2011 relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case COMP/39.592 - Standard & Poor's)* (hereinafter "Commission Decision of 15.11.2011"), available at: http://ec.europa.eu/competition/antitrust/cases/dec_docs/39592/39592_2152_5.pdf

[5] See *Commission Decision of 20.12.2012 addressed to: Thomson Reuters Corporation and Reuters Limited relating to a proceeding under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the EEA Agreement (Case COMP/39.654 – Reuters Instrument Codes (RICs))*, available at: http://ec.europa.eu/competition/antitrust/cases/dec_docs/39654/39654_2861_16.pdf

direct and indirect users of the relevant identification codes to switch providers more easily and to avoid paying uncompetitive fee rates for the relevant services.

EU legislators and supervisory authorities should take these competition issues into account in the development of regulatory approaches to FinTech, for example by:

a) requiring trading venues and data service providers to provide services at fair and reasonable prices;[6]

b) requiring trading venues and data service providers to allow third parties to access the data (in the cloud or otherwise) for purpose of facilitating the use of FinTech solutions; and

c) prohibiting anti-competitive contractual provisions, such as obligations on firms that use the relevant data to purge the data from their applications on termination of their agreement with the provider.

This is an area that warrants further consideration by policy makers and investigation by the Commission's Directorate General for Competition.

Confidentiality and data security standards of regulatory authorities

The ability for regulatory authorities to preserve the confidentiality and maintain the security of commercially sensitive information and proprietary data is one of the most significant concerns for asset managers in developing and utilising FinTech solutions and in sharing with regulators the information relating to such solutions. We urge regulatory authorities to exhaust all other oversight possibilities before resorting to requests for confidential intellectual property. See further our response to Question 1.3 (above) in relation to algorithmic source codes and our response to Question 4.7 (below) in relation to cyber security standards and resources of regulatory authorities.

It is a prerequisite to market confidence and to the successful implementation of FinTech solutions in the EU that EU and member state supervisory and regulatory authorities are able to protect the confidentiality of proprietary and other sensitive information reported by market participants, particularly in light of the vast amounts of such information that regulated entities are required to report. Over the past decade, the amount and sensitivity of information being reported to regulators has increased dramatically. However, information security and cyber intrusion and theft have become among the greatest threats to public institutions, private companies, and to the global economy. The public and private-sectors alike have become more sensitive to the risk of cyber espionage and the real potential that in the wrong hands, sensitive information could damage market participants and capital markets.

For example, MFA was particularly concerned that the Dutch AFM had inadvertently published, on its website, sensitive confidential data about certain hedge funds' short positions for

[6] *See* Commission Decision of 15.11.2011, supra footnote 4 at p. 8 (citing Article 102(a) of the Treaty on the Functioning of the European Union as stating that an abuse of a dominant position may, in particular, consist in "directly or indirectly imposing unfair purchase or selling prices;" and citing to the Court of Justice of the European Union that a price is excessive where it "has no reasonable relation to the economic value of the product supplied.").

several days.[7] Similar inadvertent data breaches have occurred in the US and other jurisdictions.

In light of these increasing risks, we believe it is critical that specific confidentiality protections be included within legislation and regulation that requires reporting of sensitive, confidential information from market participants. For example, we believe the confidentiality safeguards set out in Article 76 of the MiFID II Directive should incorporate specific references to data security and a specific confidentiality obligation for trading venues, given the vast amounts of data now collected by such venues (including, for example, on commodity derivative positions of market participants). We further believe that regulators tasked with collecting sensitive and confidential information should establish robust procedures and protocols designed to protect such information from theft and inadvertent disclosure. MFA members have significant experience in dealing with the protection of their own sensitive information from cyber and other similar risks and we stand ready to work with the Commission and other regulators in developing strong protections for confidential information.

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

The use of technology to facilitate regulatory reporting of investment funds and their managers is arguably the most promising near-term use case of RegTech in the asset management industry. At the same time, asset managers are now turning to RegTech (including artificial intelligence - e.g. the use of natural language processing) to fulfil their regulatory monitoring obligations, for example under the Market Abuse Regulation and, from January 2018, under MiFID II.

Technological solutions for regulatory reporting, including those involving DLT, can improve the efficiency of such processes and ultimately the accuracy of reports submitted to regulators and the timeframes within which firms are able to produce such reports. However, the EU financial services regulatory framework has not mandated any efficient ways for firms to submit reports; variations in reporting processes between member states and across EU regulatory regimes pose significant challenges to firms seeking to utilise such RegTech solutions.

Improving reporting processes

Regulators could and should do more to make reporting processes more efficient. Many reporting processes of EU member state competent authorities are inefficient and inconsistent with those of other competent authorities, and do not permit submission of reports in easily searchable machine-readable formats. For example, member states have different requirements with respect to the reporting of net short positions under Regulation (EU) No 236/2012 on short selling and credit default swaps (the "SSR"), with at least one jurisdiction (the Netherlands) requiring firms with a reportable short position to physically sign a form, email a PDF file to the regulator, and then post a hard copy of the signed form.

These cumbersome, duplicative, and variable processes undermine the ability of firms to utilise RegTech solutions to produce and submit reports, which creates inefficiencies and can lead to inadvertent reporting errors and inaccuracies. Competent authorities should harmonise their processes

[7] https://www.bloomberg.com/news/articles/2017-01-26/dutch-regulator-accidentally-posted-soros-s-short-positions.

and invest in their reporting processes to ensure that firms are able to submit reports efficiently and in formats that facilitate RegTech solutions.

Centralised and standardised mechanisms of reporting, for example through the European Securities and Markets Authority ("ESMA"), could greatly improve efficiency in this regard. Such mechanisms would also be more cost-effective for regulators as they would obviate the need for each EU member state competent authority to develop and maintain their own IT infrastructures for the collection of regulatory reports. Given these cost savings, national regulatory authorities could be required to provide financial support to ESMA for the development and maintenance of such centralised mechanisms. This is an area that would warrant specific public consultation given the number of firms affected and the importance of the issue.

Harmonising regulatory reporting regimes

MFA supports effective and cohesive reporting requirements that enable authorities to monitor the markets effectively for abusive behaviour and for systemic risk. However, market participants continue to have difficulty analysing and implementing the inconsistent reporting requirements under the SSR, as described above. Market participants also have difficulty analysing and implementing the overlapping reporting requirements under MiFID II, Regulation (EU) No 648/2012 on OTC derivatives ("EMIR"), Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency ("REMIT") and Regulation (EU) 2015/2365 on securities financing transactions (the "SFTR"). Each of these reporting regimes applies in a slightly different manner in terms of a number of important issues, including: (1) content; (2) which entity has the obligation to report; (3) the ability to delegate; (4) permitting single-sided reporting of transactions; and (5) back-loading.

In our view, all four reporting regimes should be harmonised to the greatest extent possible, to reduce the operational burden for market participants.[8] We also continue to encourage the Commission to adopt single-sided reporting across all four regimes. A single-sided reporting framework would be beneficial to both transaction counterparties and their regulators, given that it would eliminate the problems associated with ensuring that the data in transaction reports matches. Reducing the unnecessary regulatory uncertainty and operational burdens that result from the different reporting obligations would be a valuable improvement to market participants that invest across EU capital markets, while continuing to provide European regulators with the information they need to fulfil their obligations.

Harmonised reporting would better facilitate the use of RegTech solutions to improve efficiency and accuracy. It would also facilitate regulatory review and analysis of the reported information as regulators will better be able to compare data provided on various reports.

Creating a centralised databases for reporting purposes

Another area of regulatory reporting that could be improved to facilitate the use of RegTech

[8] See further the section headed "Issue 6 - Reporting and disclosure obligations" (pp. 31-38) in MFA's response letter of January 30, 2016 to the European Commission's *Call for Evidence in relation to the EU regulatory framework for financial services*, available here: https://www.managedfunds.org/wp-content/uploads/2016/02/MFA-Response-to-CMU-Call-for-Evidence1.pdf.

solutions is the establishment of centralised, approved databases that firms can access to comply with regulatory reporting regimes. SSR reporting, for example, is very cumbersome and time-consuming for two main reasons:

1. There is no definitive source of information on which firms can rely to determine which securities are subject to the SSR. There is an ESMA database of shares admitted to trading ("ESMA Shares Admitted Database") and another for shares exempted from the SSR ("ESMA Exempted Shares Database"). However, shares listed on a multilateral trading facility ("MTF"), to which the SSR applies, are not included in the ESMA databases. As a result, firms cannot rely solely on the ESMA databases and instead need to spend a lot of time trying to determine whether a particular security is subject to the SSR. For example, there have been cases of issuers with significant liquidity outside the EU that are listed on an MTF and are not included on the ESMA Shares Admitted Database (e.g., GW Pharmaceuticals plc (ticker GWPH)). A firm can easily fail to realise it has an SSR obligation with respect to these securities even if it is trying to be compliant by reviewing the ESMA Shares Admitted Database, especially if the firm only trades securities listed in third countries and is not as familiar with all the nuances of the SSR regime.

2. There is no definitive source of information on which firms can rely with respect to shares outstanding. The SSR uses a non-market-standard definition of shares outstanding (aggregating all classes of shares, including treasury shares, etc.). As a consequence, there is no commercial source a firm can use to determine the correct figure for shares outstanding. This means that a firm must use a different source for the information for each member state, and in many jurisdictions (including, France, Germany and Italy, among others) there is no one "definitive" source of such information. This makes the task for firms acting in good faith to meet their obligations under the SSR extremely challenging, particularly where corporate actions are taking place that may affect the relevant figures.

Without an accurate, approved centralised database of shares subject to SSR and issued share capital, firms must employ people to carry out laborious searches, which is an inefficient and not always accurate process. Creation of a central data source, operated for example by ESMA, would better enable firms to utilise RegTech solutions to improve efficiency and accuracy of reporting of net short positions under the SSR. Alternatively, ESMA could authorise reporting firms to rely on third-party databases.

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?

In order for the asset management industry to make full and effective use of DLT solutions in the EU, market participants need assurance that the relevant regulatory frameworks require DLT network operators, trading venues and CCPs to adhere to robust standards of governance, data protection and network security.

Governance

First, to the extent EU financial markets move towards private DLT networks, we believe the governance structure of such networks will be important in promoting fair, efficient and open markets, and for ensuring that a DLT network is operated for the benefit of the public good. To that end, we believe it is important for the European Commission and the other EU legislative institutions and supervisory authorities to seek to ensure that the governance structure for a DLT network includes buy-side representation and that the governance process is sufficiently transparent to address potential conflicts of interests.

Data protection

Second, we believe that the EU legislators and supervisory authorities need to ensure that the use of DLT does not undermine protections regarding personal information or the confidentiality of investors' orders, positions or trading strategies. We appreciate that DLT has the potential to promote increased transparency. Nevertheless, it is imperative that DLT networks are designed in ways that keep certain transactional and position information anonymous and private. Disclosure of such information would be detrimental to investors, negatively impact financial markets, and impair confidence in EU regulatory frameworks.

Network Security

Security is a critical consideration for a DLT network. We urge EU legislators and supervisory authorities to hold network operators, trading venues and CCPs to rigorous standards with respect to network and data security, and to ensure that network operators dedicate adequate resources towards maintaining and enhancing data security. As demonstrated over the last few years, including the recent malware attacks, no entity is immune from cyberattacks and the number and level of attacks have only increased. In the cyber era, we believe security standards need to be robust and take into consideration the very real threat of an attack from individuals, organised groups, and even nation states.

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?

As discussed in our response to Question 2.4, the ability for firms to utilise RegTech solutions to improve the efficiency and accuracy of regulatory reporting of transactions would be greatly enhanced if:

- regulatory reporting processes were harmonised and made more efficient;
- the reporting requirements under MiFID II, EMIR, REMIT and the SFTR were harmonised; and
- central databases of common information needed for regulatory reporting were made available to firms to facilitate such reporting.

As discussed in our response to Question 2.2 above, confidentiality safeguards set out in

Article 76 of the MiFID II Directive should incorporate specific references to data security and a specific confidentiality obligation for trading venues, CCPs, and other financial intermediaries.

In a similar vein, data security and confidentiality practices of EU and member state authorities is another area in which supervisory practice should be adapted to facilitate implementation of FinTech solutions. As discussed in our responses to Question 1.3 (above) and Question 4.8 (below), the ability for such authorities to protect sensitive firm data from cyber security threats poses a challenge to firms in developing FinTech solutions and cooperating with regulators to tackle cybersecurity threats.

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

MFA supports the Commission's principles of technological neutrality, proportionality and integrity. As regards proportionality, it is important that the regulatory approach to FinTech activities in the asset management sector differentiates between retail investors, who require greater levels of regulatory protection, and sophisticated professional investors, which are generally better equipped to assess for themselves the performance and standards of their asset managers.

Pursuant to the principles of technological neutrality and proportionality, the Commission should encourage principle-based regulation of FinTech, rather than prescriptive regulatory rules. Principle-based regulation is an appropriate basis for regulating FinTech activities given the rapid pace of technological change and the variety of FinTech solutions and the market participants that utilise them. Such an approach would be in keeping with prevailing regulatory practices in third countries.[9]

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

As discussed in our response to Question 2.4 above, harmonisation of EU regulatory reporting regimes would facilitate greater efficiency and interoperability of FinTech solutions in the areas of automated advice and trading and the use of FinTech solutions in outsourcing arrangements respectively.

EU legislators and authorities should coordinate with third country legislators and regulatory authorities through international regulatory bodies and standard-setting organisations to limit duplicative and inconsistent regulatory requirements on firms.

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

Please see our response to Question 2.9 (above) regarding the need for DLT operators to be

[9] For example, the U.S. Commodity Futures Trading Commission ("CFTC") recently adopted an amendment to its recordkeeping Rule 1.31 that modernizes the regulation by making technologically neutral the form and manner in which regulatory records must be kept. Prior to its amendment, CFTC Rule 1.31 required the use of technology that had become outdated, creating a potential security threat. See *CFTC Final Recordkeeping Rule, 82 Fed. Reg. 24,479 (May 30, 2017)*, available at: http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2017-11014a.pdf.

subject to robust data protection standards. In addition, it is appropriate for the EU to periodically reconsider the extent and degree of information collected, which will always be vulnerable to theft and misappropriation. For example, MiFID II requires firms to provide extremely sensitive personal information of investment staff (e.g. national insurance numbers or passport numbers) in every transaction report. Such information will be very attractive to thieves and may be pursued for identity theft, financial crimes, and the production of false documents, among other crimes. It will be available to wide numbers of people and in a myriad of systems, all of which will be vulnerable to theft and cyber-attacks. In this regard, policy makers and regulators should consider whether such reporting requirements are necessary and proportionate to their public policy objectives given the data protection risks they create. In particular, limiting the requirements to report such sensitive data to firms that have committed a regulatory breach would be a much more proportionate and risk-sensitive approach.

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?

Cyber-security standards for financial services firms are important for ensuring the integrity of financial markets. Given the pace of technological change and of new emerging cyber security threats, it is important that such standards are principle-based rather than detailed prescriptions of the actions required of firms. Cyber threats do not respect national borders and in this regard international cooperation is paramount. EU supervisory authorities and the competent authorities of EU member states should cooperate with regulators in other jurisdictions to assess and respond to cyber security threats and principle-based standards should be developed at the EU-level with regard to the standards applicable in other jurisdictions. Such standards should avoid requirements that are duplicative of, or conflict with, requirements in third countries such as the United States.

At least equally important to the cyber-security standards applicable to financial service providers are those applicable to regulatory and supervisory authorities and to their service providers. Such authorities and service providers are at least, if not more, susceptible to cyber attacks then are regulated firms. They are also likely to be in possession of a far greater volume of sensitive data than any individual regulated firm. Consequently, from the perspective of a malware creator or hacker, regulatory authorities and their service providers may be seen as a soft target and the impact of a data security breach of such authorities or their service providers on financial markets is likely to be far higher. In this regard it is crucial that the EU supervisory authorities and the competent authorities of EU member states invest in effective up-to-date cybersecurity measures and impose robust standards on their external service providers, particularly those engaged in regulatory reporting processes.

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?

Concerns among financial service providers about the abilities of supervisory and regulatory authorities to protect the confidentiality and security of information impede cyber threat information sharing. Such concerns could be addressed by bolstering cyber security standards and resources of such authorities. See further our responses to Questions 2.2 and 4.7 (above).

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)?

MFA supports coordination among regulators to address cybersecurity threats. See further our response to Question 4.7 (above). Harmonised principle-based standards and mutual recognition of resilience testing across the EU would increase the efficiency and effectiveness of cybersecurity measures and reduce the risk of cyber criminals identifying certain EU member states as 'soft-targets' for attacks. Such harmonisation and regulatory coordination is also important to enable firms to design and maintain global cyber security programmes that comply with standards in multiple jurisdictions, including third country regimes.