European Securities and Markets Authority

29 June 2020
ESMA50-164-3463

ESMA's response to the European Commission's Consultation on a New Digital Finance Strategy for Europe

Introduction

ESMA welcomes the opportunity to respond to the European Commission's Consultation on a New Digital Finance Strategy for Europe (hereafter "the Consultation").[1] ESMA's response, which was submitted to the Commission on 26 June 2020, is set out below.

General questions

Question 1. What are the main obstacles to fully reap the opportunities of innovative technologies in the European financial sector (please mention no more than 4)? Please also take into account the analysis of the expert group on Regulatory Obstacles to Financial Innovation in that respect.

Innovative technologies are rapidly transforming the way in which the financial sector operates. Data analytics, machine learning, cloud computing and Distributed Ledger Technology are examples of new technologies that have the potential to help bring faster, more transparent, more efficient financial services to consumers, possibly at a lower cost.

The existing regulatory framework was not necessarily designed with these innovative technologies in mind, which creates a range of challenges for both firms and regulators/supervisors. These challenges are mainly threefold:

- First, there may be a **lack of clarity** as to whether and exactly how the existing rules may apply to innovative business models and processes. Different interpretations on the part of firms and across national supervisors may create inconsistencies and fragmentation in the EU.

- Second, some **adaptations may be needed** to allow for an effective application of the existing rules, for example when new technologies make certain operating processes redundant, or to address the new or exacerbated risks introduced by these new technologies;

[1] https://ec.europa.eu/info/consultations/finance-2020-digital-finance-strategy_en

- Third, these new technologies are typically global and therefore require a **coordinated response** at EU and international level.

Firms and, regulators/supervisors may also face challenges in building the **necessary knowledge and expertise** to fully reap the benefits of these technologies, bearing in mind that the development and adoption of such technologies is often resource intensive.

In addition, there may be a deficit of **digital financial literacy on the part of consumers/investors**, with potential detrimental effects on investor protection and financial inclusion. In particular, consumers/investors may not fully understand the complexity and the risks involved in such technologies. Also, certain categories of consumers/investors, e.g., elderly people, may not have the necessary skills or resources to make the best use of the technologies.

Against this background, regulators need to take an active approach to make sure that their rules remain fit for purpose and that they understand the business cases at hand. The regulatory framework should not unduly restrict potentially beneficial innovations but, at the same time, not leave risks unaddressed. An **EU-wide harmonised regulatory/supervisory framework** is necessary to both allow innovative firms in the EU to reach the scale that they need and provide for the necessary safeguards to investor protection, financial stability and orderly markets. In this context, the concept of technological neutrality should apply.

Finally, there is a need to balance the digital rights of consumers and firms' employees with the needs of supervisors and regulators to have sufficient access to data used by firms.[2]

Question 2. What are the key advantages and challenges consumers are facing with the increasing digitalisation of the financial sector (please mention no more than 4).

For each of them, what if any are the initiatives that should be taken at EU level?

There are many possible drivers of digitalisation, including cost-cutting, automation or an aim to improve service quality. Accordingly, different instances of financial services digitalisation may create different advantages and challenges for consumers. An additional caveat is that recent responses to the Covid-19 crisis have accelerated the trend to digitalisation in certain areas. A rapid adjustment of this kind may have consequences that are not yet apparent, suggesting that ongoing monitoring is advisable. The following list of advantages and challenges is therefore not exhaustive.

Advantages of digitalisation include:

- **A potential increase in the quality, speed and convenience of financial services** provision. While AI applications are just one aspect of the broader trends of

[2] Recommendations 13, 25, 26 and 27 of the Report on Regulatory Obstacles to Financial Innovation expand upon this issue.

digitalisation, they provide some instructive examples. For instance, they can help firms to better identify customers' needs and to better tailor their services to specific client groups. Additionally, digitalisation can allow consumers to inform themselves about their financial services from home or a mobile terminal (e.g. via various search engines).

- **Possible improvement of fraud detection**. Especially through rule-based or more enhanced AI-based tools, firms can enhance the efficiency of their anti-money laundering and Know-Your-Customer (KYC) verifications. This may improve the detection of fraud (attempts) and increase the safety of using financial services for consumers.

- **Potentially increased access** to financial services: Applications such as automated advice can simplify consumers' access to different asset markets for their investments

- Cross-border business can generate economies of scale, which can in turn lead to **lower costs**.

Challenges include the following.

- Managing **risks around data security and privacy** is likely to be a major challenge as individuals have increasing amounts of personal data and financial data held by different financial service providers and by providers that offer cross-sectoral platforms to consumers. Cybersecurity risks are an area of growing concern due to their increasing frequency and impact. Data security breaches can be severely detrimental to consumers and may even undermine trust in the wider financial system.

- **Potentially detrimental price optimisation/discrimination and sales practices**. As a by-product of digitalisation, a lot of data is created which can be used for other applications such as big data analytics. Big data analysis allows firms to gain more detailed insights on (non-risk related) consumer preferences such as willingness to pay or customer inertia and nudge them in another direction. Consequently, the risk of unfair consumer treatment may increase, e.g. via offering the same service at diverging prices, depending on consumer behaviour ("price optimisation"). This may lead to consumer detriment, if financial service providers systematically exploit consumers' biases or constraints such as limited time or (lower) financial knowledge. The risk of customers being unfairly treated may increase if raw data is based on human interactions that are themselves subject to (conscious or unconscious) bias.

  A related risk is that firms may ask more information than needed to provide a service so that they can sell the data/use it for other purposes such as price optimisation. In more extreme cases, such behaviour may amount to a form of misconduct. Another area of risk to consumers that may arise from increasing digitalisation is around cross-selling, including the risk that the sale of a product or service is made contingent on the consumer purchasing another product or service from that firm. This issue may become especially relevant as large technology firms, who already providing technology

services to consumers, enter financial services. Finally, some online environments may encourage rushed decision-making, exacerbating behavioural biases.

- **Lack of transparency.** Depending on the models used, it can be difficult to provide an explanation of an algorithm-based investment or lending decision to consumers, for example, if the latter challenge it. Moreover, a lack of transparency may make it hard to detect technical problems (e.g. biases of the algorithm) which may have a detrimental impact on the provision of financial services to consumers.

- **Some consumers may suffer reduced access** if they are not comfortable using online services, and these services 'crowd out' traditional modes of provision. In addition to the fundamental challenge posed by financial illiteracy and unfamiliarity with digital technologies, there is a risk that innovative digitized products can in some cases involve additional complexity around financial products and services.

Question 3. Do you agree with the choice of [the following] priority areas?

1. **ensuring that the EU financial services regulatory framework is technology-neutral and innovation friendly;**
2. **reaping the opportunities offered by the EU-wide Single Market for digital financial services for consumers and firms;**
3. **promoting a data-driven financial sector for the benefit of EU consumers and firms; and**
4. **enhancing the operational resilience of the financial sector.**

Yes.

Question 3.1 Please explain your answer to question 3 and specify if you see other areas that would merit further attention from the Commission.

It is important to keep in mind that new technologies and digitalisation are reliant on data and may provide benefits only to the extent that they are cyber resilient, meaning that the four priorities are closely interrelated.

In the first priority area, promoting innovation while ensuring that the regulatory framework does not favour certain technological choices over others may be a delicate balance in certain cases, e.g. if a given innovation involves a particular type of technology.

For the second priority area, the extent to which consumers will benefit from digitalisation depends on their financial and digital literacy (which extends to their understanding of data privacy and data security risks).

For the third priority area, a data-driven financial sector may require enhanced supervisory capabilities and expertise.

Section I: Ensuring a technology-neutral and innovation friendly EU financial services regulatory framework

Question 4. Do you consider the existing EU financial services regulatory framework to be technology neutral and innovation friendly?

No.

Question 4.1. If not, please provide specific examples of provisions and requirements that are not technologically neutral or hinder innovation.

ESMA regards the regulatory framework as broadly technologically neutral. However, we have answered 'no' above in order to highlight some subtleties in this regard. Our work regarding Crypto-Assets (CAs) highlights examples where risks may emerge that are specific to a technology. In this sense, technological neutrality may be consistent with a regulatory approach that focuses on a specific technology. Such an approach may in principle also promote innovation-friendliness.

ESMA's assessment of the overall framework regarding technological neutrality and innovation-friendliness is based on its work in recent years. ESMA takes a balanced approach to innovation, meaning that we are both supportive of innovation that can bring benefits and protective towards the risks that new technologies may introduce. Meanwhile, we realise that some rules were not designed with these new technologies in mind. Following the 2018 European Commission's FinTech Action Plan, ESMA undertook extensive work on the relevant priority areas to foster the development of a more competitive and innovative European financial sector. This work has informed many of our answers to this consultation and is set out in more detail in our answer to question 6.1.

Our work on CAs is summarised as follows.[3]

There are a wide variety of CAs and **a 'case by case' approach** is needed when it comes to legally qualifying them. Some CAs, e.g., those with attached profit rights, are likely to qualify as MiFID financial instruments. Meanwhile, others, which represent a large portion of those CAs outstanding, are likely to fall outside of the existing EU financial securities rules.

Where CAs qualify as MiFID financial instruments they should be regulated as such. However, applying the existing rules to these novel instruments reveals several gaps and issues in the existing rules:

[3] Please note that more details on the outcomes of ESMA work on CAs is available in the ESMA Advice on ICOs and CAs published in January 2019 (available at: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf). In particular, the Advice represents a comprehensive assessment of the applicability of the existing EU financial securities rules to CAs. It also involved an extensive survey to NCAs on the legal qualification of CAs, the results of which were published alongside the Advice.

- First, ESMA believes that greater clarity around the types of services/activities that may qualify as custody/safekeeping services/activities under EU financial services rules in a DLT framework is needed. Also, there may be a need to consider some 'technical' changes to some of the existing requirements in relation to custody/safekeeping services/activities as they may not be adapted to DLT technology.

- Second, greater certainty around the concepts of settlement and settlement finality applied to CAs is needed. ESMA believes that there may be a need to distinguish between permissioned and permissionless DLTs in that respect. In particular, ESMA has identified specific governance issues with permissionless DLTs, which makes them less suitable to the processing of financial instruments, at least in their current form. A related issue is the role of 'miners' and how they would be handled under the existing rules given their novel and fundamental role in the settlement process. Another important element to consider is how to achieve Delivery versus Payment (DvP) especially if there is a cash leg that is not processed on the DLT. In connection to this, the provision of settlement in central bank money, where practical and available, should also be analysed.

- Third, ESMA has identified risks that are specific to the underlying technology that might require new/enhanced requirements. In particular, ESMA believes that there should be a means to ensure that the protocol and smart contracts underpinning CAs meet minimum reliability and safety requirements. More generally, cybersecurity risks, including the risks of hacks, posed by DLT should be considered, to assess whether they are appropriately addressed by the existing set of rules.

- Other gaps and issues that would require consideration include the lack of clarity on how to apply the existing rules to so-called decentralised and hybrid models using so-called 'smart contracts' and the need to make some adaptations to certain existing pre- and post-trade transparency and data reporting requirements.

- Also, Member States NCAs in the course of transposing MiFID into their national laws, have in turn defined the term financial instrument differently. While some employ a restrictive list of examples to define transferable securities, others use broader interpretations. This creates challenges both in the regulation and supervision of CAs.

Where CAs do not qualify as MiFID financial instruments, there are important risks, including to investor protection, and EU policymakers should consider possible ways to address these risks in a proportionate manner.

In addition, while the findings of the ESMA Advice remain valid, ESMA believes that market developments in relation to CAs should be monitored closely, as this is a constantly evolving area. In particular, ESMA believes that the recent developments around so-called stablecoins require close scrutiny, including at international level, considering their potential to reach a large scale quickly and the risks that they may pose to financial stability.

Question 5. Do you consider that the current level of consumer protection for the retail financial products and services established by the EU regulatory framework is technology neutral and should be also applied to innovative ones using new technologies, although adapted to the features of these products and to the distribution models?

Yes.

Question 5.1 Please explain your reasoning on your answer to question 5, and where relevant explain the necessary adaptations.

In general, the EU regulatory framework around consumer (i.e. retail investor) protection appears to be technology neutral. That said, ESMA's work on CAs/DLT and the resulting Advice of January 2019 (see answer to question 4.1) highlights some specific issues relevant to consumer protection. ESMA agrees that existing frameworks should in general be applied according to the features of innovative products and distribution models, rather than specific to the technology itself. (However, in some cases an innovative product or distribution model may have features that arise from a new technology, e.g. DLT.) The approach described in question 5 sounds technologically neutral in this general sense, a principle that ESMA supports.

Question 6. In your opinion, is the use for financial services of the new technologies listed below limited due to obstacles stemming from the EU financial services regulatory framework or other EU level regulatory requirements that also apply to financial services providers?

Key: 1 – irrelevant. 2 – rather not relevant. 3 – neutral. 4 – rather relevant. 5 – fully relevant.

DLT (except crypto-assets)	4
Cloud computing	2
Artificial Intelligence / Machine Learning	3
Internet of Things (IoT)	2
Biometrics	2
Quantum computing	1
Other	N/A

Question 6.1. Please explain your answer to question 6, specify the specific provisions and legislation you are referring to and indicate your views on how it should be addressed.

The answer to question 6 is based on work that ESMA has undertaken. ESMA takes a balanced approach to innovation, meaning that we are both supportive of innovation that can bring benefits and protective towards the risks that new technologies may introduce. Meanwhile, we realise that some rules were not designed with these new technologies in mind. Following the 2018 European Commission's FinTech Action Plan, ESMA undertook extensive work on the five priority areas listed below. In addition, ESMA has undertaken significant work on DLT. In June 2017, ESMA published a DLT report highlighting the potential benefits and risks of the technology applied to financial securities markets.[4] The report did not highlight any major impediment in the EU framework that would prevent the development of the technology. Yet we identified a series of issues that would require further consideration, as the technology develops.

1. **Crypto-Assets (see answer to question 4.1).**

The ESMA 2019 Advice on ICOs and CAs followed up on the aforementioned work on DLT.

2. **Licensing requirements**

ESMA conducted two Surveys to gather evidence from NCAs on the licensing regimes of FinTech firms in their jurisdictions. The first conducted in January 2018, sought to identify potential gaps and issues in the existing EU regulatory framework, assess how the existing national regimes diverge and, if identified, propose recommendations to adapt the EU legislation to the emerging innovations. The second, launched one year later, attempted to identify the ways in which NCAs employed the concepts of 'proportionality' and 'flexibility' when licensing FinTech firms.

The ESMA Report on licensing regimes published in July 2019 provides an overview of the key findings of the Surveys.[5] Based on the evidence gathered, ESMA concluded that at present most innovative business models can operate within the existing EU rules. Regarding CAs/ICOs/DLT and cybersecurity, ESMA reiterated the conclusions made in its 2019 pieces of Advice (see answer to question 4.1 and point 5 below).

3. **Innovation facilitators**

In December 2018, ESMA together with the EBA and EIOPA submitted to the Commission the Joint ESA Report on regulatory sandboxes and innovation hubs.[6] The Report provides a comparative analysis of innovation facilitators in Europe focusing on two types of innovation

[4] https://www.esma.europa.eu/press-news/esma-news/esma-assesses-dlt's-potential-and-interactions-eu-rules
[5] https://www.esma.europa.eu/sites/default/files/library/esma50-164-2430_licensing_of_fintech.pdf
[6] https://www.esma.europa.eu/press-news/esma-news/esas-publish-joint-report-regulatory-sandboxes-and-innovation-hubs

facilitators, namely 'innovation hubs' and 'regulatory sandboxes', and sets out 'Best Practices' regarding the design and operation of innovation facilitators.

Following this Report, the Commission, together with the ESAs and NCAs, launched under the Joint Committee of the ESAs the European Forum for Innovation Facilitators (EFIF) on 2 April 2019. The EFIF provides a platform for supervisors to meet regularly to share experiences from engagement with firms through innovation facilitators, to share technological expertise, and to reach common views on the regulatory treatment of innovative products, services and business models. The main objective of the EFIF is to promote coordination and cooperation among national innovation facilitators to foster the scaling up of innovation in the financial sector.[7] The concept of an innovation hub has continued to evolve any can now include support and advice services, access to investor networks and accelerators. Continual monitoring is warranted.

Following the launch, the EFIF met in September 2019, December 2019 and April 2020. The meetings included a tour de table of NCAs to take stock of new developments at national level and presentations from firms on their experience in using innovation facilitators, with a specific focus on CAs, stablecoins and DLT; Artificial Intelligence and Big Data; and platformisation.

4. Cloud services

ESMA has recently launched a consultation paper on proposed guidelines on outsourcing to cloud service providers.[8]

The guidelines aim to provide guidance to firms and competent authorities to help them identify, assess and monitor the risks arising from the use of cloud in a relevant manner. Importantly, the proposed guidelines are consistent with the guidelines already published by EBA and EIOPA, as indeed a consistent approach is paramount considering the cross sectoral nature of cloud computing.

Upon receiving feedback to the consultation, ESMA expects to publish final guidelines on cloud outsourcing in Q1 2021.

5. Cyber resilience

ESMA and the other ESAs published joint Advice in April 2019 on two cybersecurity-related topics: (1) Advice on legislative improvements relating to ICT risk management requirements in the EU financial sector, and (2) Advice on the case for a coherent EU-wide cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector. Following these publications and the consultation from the Commission on a Digital

[7] See for further details: https://esas-joint-committee.europa.eu/Pages/Activities/EFIF/European-Forum-for-Innovation-Facilitators.aspx
[8] https://www.esma.europa.eu/press-news/esma-news/esma-consults-cloud-outsourcing-guidelines

Operational Resilience framework[9], ESMA continues to work closely with international authorities, NCAs and the Commission on cybersecurity-related matters.

Question 7. Building on your experience, what are the best ways (regulatory and non-regulatory measures) for the EU to support the uptake of nascent technologies and business models relying on them while also mitigating the risks they may pose? Please rate each proposal from 1 to 5.

Key: 1 – irrelevant. 2 – rather not relevant. 3 – neutral. 4 – rather relevant. 5 – fully relevant.

Setting up dedicated observatories to monitor technological and market trends (e.g. EU Blockchain Observatory & Forum; Platform Observatory)	4
Funding experimentation on certain applications of new technologies in finance (e.g. blockchain use cases)	4
Promoting supervisory innovation hubs and sandboxes	4
Supporting industry codes of conduct on certain applications of new technologies in finance	4
Enhancing legal clarity through guidance at EU level for specific technologies and/or use cases	5
Creating bespoke EU regimes adapted to nascent markets, possibly on a temporary basis	4
Other	N/A

[9] https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf

Question 8: In which financial services do you expect technology companies which have their main business outside the financial sector (individually or collectively) to gain significant market share in the five upcoming years? Please rate each proposal from 1 to 5.

Question 8.1 Please explain your answer to question 8 and, if necessary, describe how you expect technology companies to enter and advance in the various financial services markets in the EU Member States.

Future market developments are notoriously hard to predict. ESMA continues to monitor various market trends as they emerge and has recently carried out some analysis of the implications of large technology companies entering financial services.[10] In securities markets in other regions – notably China, but also in countries in South America for example – firms whose original/core business was in online marketplaces are looking to offer money market funds to consumers. There appears to be scope for some large technology firms to develop offerings in asset management more widely. Another area of natural interest is automated advice.

Question 9. Do you see specific financial services areas where the principle of "same activity creating the same risks should be regulated in the same way" is not respected?

No.

Question 9.1 Please explain your answer to question 9 and provide examples if needed.

At present we do not see the principle being violated. However, any regulatory action to address the gaps and issues that exist in the current financial securities rules in relation to crypto-assets, including global stablecoin arrangements, would need to be carefully considered to avoid unintended consequences, e.g. undue differences in the way these instruments are treated relative to 'traditional' instruments.

[10] ESMA Report on Trends, Risks and Vulnerabilities no. 1 2020, pp. 48-59.

Question 10. Which prudential and conduct risks do you expect to change with technology companies gaining significant market share in financial services in the EU in the five upcoming years? Please rate each proposal from 1 to 5. Please specify which other prudential and conduct risk(s) you expect to change with technology companies gaining significant market share in financial services in the EU in the five upcoming years.

Question 10.1. Please explain your answer to question 10 and, if necessary, please describe how the risks would emerge, decrease or increase with the higher activity of technology companies in financial services and which market participants would face these increased risks.

ESMA has recently carried out some analysis of the implications of large technology companies ('BigTechs') entering financial services.[11] Some of these firms have dominant market positions in the services they provide, which in certain cases give them considerable power to set prices and contract terms. Their vast customer networks, data analytics and brand recognition mean they have scope to attain considerable market share in financial services in future.

Firms moving into financial services will be subject to relevant regulations. Given the data-based nature of the core business of these firms, however, we believe several changing risks should be considered.

Significantly, operational risk may change in nature as technology companies operate integrated platforms across different economic sectors. For example, an operational incident arising on a platform in respect of one line of business could impact the functioning of other lines of business, including financial services.

This change in market structure may lead to a new form of concentration risk. More broadly, interconnectedness may amplify financial stability risks associated with the entry of BigTech into financial markets. This interconnectedness may be seen in, for example simultaneous provision of services such as data analytics, cloud services and credit provision to other non-financial firms to manage their liquidity.

[11] ESMA Report on Trends, Risks and Vulnerabilities no. 1 2020, pp. 48-59.

Question 11. Which consumer risks do you expect to change when technology companies gain significant market share in financial services in the EU in the five upcoming years? Please rate each proposal from 1 to 5. Please specify which other consumer risk(s) you expect to change when technology companies gain significant market share in financial services in the EU in the five upcoming years.

Question 11.1 If necessary, please describe how the risks would emerge, decrease or increase with the higher activity of technology companies in financial services and which market participants would face these increased risks.

As noted in the answer to question 10, ESMA has recently carried out some analysis of the implications of large technology companies entering financial services. Some of these firms have dominant market positions in the services they provide, which in certain cases give them considerable power to set prices and contract terms. Their vast customer networks, data analytics and brand recognition mean they have scope to attain considerable market share in financial services in future.

Firms moving into financial services will be subject to relevant regulations. Given the data-based nature of the core business of these firms, however, we believe several changing risks to consumers should be considered.

Risks around the use and management of personal data are likely to be exacerbated by the scope for data matching across services (including non-financial services) combined with Big Data. Additionally, some relevant companies have reputational issues in this regard. For similar reasons, there may be increased scope for consumer discrimination based on profiles. The cross-sectoral nature of the business of the firms in question may pose a risk of inadequate management of conflicts of interest and risks around cross-selling.

A final area of risk to consumers relates to the extent to which technology companies may gain significant power in future over pricing and contract terms in financial services. In the short run, new entrants may drive down prices for consumers, but there is a risk that in the long run competition will suffer, raising prices for consumers. A related issue is that consumers may face greater switching costs if their use of a given financial service is integrated into a combined platform through which they access other services (including non-financial services).

However, the entry of technology companies (large or small) more broadly into financial services may also bring benefits to consumers. For example, developments in applications such as automated advice can simplify consumers' access to different asset markets for their investments.

Question 12. Do you consider that any of the developments referred to in the questions 8 to 11 require adjusting the regulatory approach in the EU (for example by moving to more activity-based regulation, extending the regulatory perimeter to certain entities, adjusting certain parts of the EU single rulebook)?

Yes.

Question 12.1 Please explain your answer to question 12, elaborating on specific areas and providing specific examples.

One development in this area on which ESMA is currently carrying out work is around firms outsourcing to Cloud Service Providers. Currently some BigTechs are entering the financial system through the provision of non-regulated financial services to a regulated entity in the form of cloud service provision. As a small number of companies represent much of the market, there is the potential for concentration risk from a system-wide perspective.

As discussed above (see answer to question 6.1), and relevant to an entity-level perspective, ESMA recently launched a consultation paper on proposed guidelines on outsourcing to cloud services providers. These guidelines will provide guidance to firms and competent authorities to help them identify, assess and monitor the risks arising from the use of cloud in a relevant manner. Based on feedback received to its consultation, ESMA expects to publish final guidelines on cloud outsourcing in Q1 2021.

In addition, ESMA believes that the recent developments around so-called stablecoins require close monitoring, including at international level, considering their potential to reach a large scale quickly and the risks that they may pose to financial stability.

Question 13. Building on your experience, what are the main challenges authorities are facing while supervising innovative/digital players in finance and how should they be addressed? Please explain your reasoning and provide examples for each sector you are referring to (e.g. banking, insurance, pension, capital markets).

Innovation/digitalisation in finance is a fast-developing area, involving new products and solutions that may go beyond traditional models and approaches. Therefore, monitoring, analysing and assessing risks and benefits of emerging innovations in the securities markets is a resource- and capacity-intensive task for supervisors. ESMA has observed the following challenges related to supervising innovation/digitalisation in the securities market.

1. Delineating the regulatory perimeter. The nature of market participants and of the activities they undertake (unregulated and regulated FinTechs, incumbents and start-ups, financial service providers or providers of technological solutions to other firms) makes it challenging for regulators and supervisors to map innovative business models, define the regulatory perimeter and properly capture innovative/digital players. For example, according to the 2018 ESMA Survey (the results of which are analysed in the ESMA Report on Licensing of FinTech Business Models), the majority of NCAs did not

identify innovative business models in their jurisdictions that are not captured by the existing authorisation/licensing requirements and that might present risks. Seven NCAs considered however that there are innovative business models that might represent risks and therefore should be captured at the EU level.

A recent development has been the entry of BigTechs into finance. These large technology companies often operate in different sectors and jurisdictions. Some of their activities may fall outside of the regulatory sphere. This structural feature may complicate the task of supervision and points to a possible need to review the perimeter of the current regulatory framework.

2. Divergences across member states' regulations. Since digital solutions typically propose or facilitate cross border activities, the diverging regulatory requirements at national levels and national specificities for authorizing/licensing innovative business models remain the key barrier for cross border activities and can hamper deployment of innovative solutions.

3. Ensuring a level playing field. Not all existing legal requirement may be easily applied to innovative/digital solutions and thus the risks inherent to these technologies may be left unaddressed (with regards to data protection and admissibility of evidence to court; related cybersecurity risks) or addressed unequally across the providers of such solutions. Safeguards for equal treatment should be ensured to facilitate competition in the market.

4. Coordinating supervisory actions with other sectoral authorities. Supervising digital technologies may involve participation of other regulators/supervisors at the national or EU level (e.g. data protection or competition authorities) and smooth procedures and decision making should be ensured.

5. Developing in-house or outsourced talent and capacities. To understand the risks and benefits of a technology, supervisors and regulators need to engage experts with adequate knowledge and skills. Maintaining a proper level of expertise is resource intensive. Authorities see benefits in developing SupTech solutions to better and more efficiently conduct supervisory and regulatory tasks.

Question 14. According to you, which initiatives could be put in place at EU level to enhance this multi-disciplinary cooperation between authorities? Please explain your reasoning and provide examples if needed.

ESMA continually works with NCAs to coordinate efforts in this area. Across the financial sector at EU level, the ESAs continue to coordinate their work through the Joint Committee of the ESAs (JC) In addition, cross-sectoral coordination could be further enhanced by working together with sectoral authorities such as the European Data Protection Board and competition agencies.

Within this context, ESMA notes that the European Forum for Innovation Facilitators (EFIF) established under the JC provides a platform for supervisors to meet regularly to share experiences from engagement with firms through innovation facilitators, to share technological expertise, and to reach common views on the regulatory treatment of innovative products, services and business models. Continuing work through EFIF will contribute to its objective of promoting coordination and cooperating among national innovation facilitators to foster the scaling up of innovation in the financial sector. To ensure close coordination, EFIF work should be aligned with other ESA and JC workstreams and fora.

National innovation facilitators remain the appropriate level for authorities to handle questions from individual firms. EFIF representatives can bring any broader issues to the Forum as they see fit.

Section II: Removing fragmentation in the single market for digital financial services

Question 17. What should be done at EU level to facilitate reliance by financial institutions on digital identities gathered by third parties (including by other financial institutions) and data re-use/portability? Please rate each proposal from 1 to 5.

Please specify what else should be done at EU level to facilitate reliance by financial institutions on digital identities gathered by third parties (including by other financial institutions) and data re-use/portability.

ESMA notes the Commission's data strategy highlights the importance of electronic identification initiatives including eIDAS. Within ESMA's remit, electronic identification is relevant in the context of customer and firm-to-firm interactions, as well as for the publication of documents such as KIIDS, KIDs, prospectuses and annual accounts.

The key prerequisite for the wide reliance on digital identities is the introduction of a unique standardised and harmonised means of identification. Such means already exist in the financial sector – ISO 10962 Legal Entity Identifier (LEI), which is a global standard. It should be promoted and exploited to the maximum extent possible while avoiding the introduction and exploitation of other competing identifiers. Identification is impeded by any form of competition between various identifiers/identities attributed to the same entity. If there are competing ways to identify an entity, this makes the respective identification processes inefficient, and likewise for subsequent data sharing and portability.

Question 18. Should one consider going beyond customer identification and develop Digital Financial Identities to facilitate switching and easier access for customers to specific financial services?

Should such Digital Financial Identities be usable and recognised throughout the EU?

ESMA believes that it would be important to develop Digital Financial Identities (DFIs) which are usable and recognised throughout the EU.

One very relevant use case for DFIs is the signature of electronic reports prepared by public companies, such as Annual Financial Reports prepared in the European Single Electronic Format (ESEF) introduced by Regulation EU 2019/815. ESMA believes that the security of information is an essential dimension of the digitalisation challenge and that electronic signatures would contribute to create trust in the information disclosed by companies in digital format. The availability of DFIs, for instance, would enable the involvement of auditors with digital reports in ESEF format in a harmonised way across the EU.

ESMA thinks that DFIs should rely on a unique standardised and harmonised means of identification, of which the LEI code is a necessary component. A proof of concept has been developed by the Global LEI Foundation in close cooperation with XBRL International in the context of the preparation of GLEIF's Annual Financial Report in iXBRL format. It was published on GLEIF's website in June 2020.[12] ESMA invites the Commission to consider such initiatives in further work relating to DFIs.

On a different note, while DFIs would bring many benefits, from an AML/CFT perspective their creation will not remove all of the due diligence obligations of an obliged entity in respect of its customers. Likewise, the introduction of DFIs should not signal a move away from a risk-based approach to AML/CFT.

Some Member States have restrictions regarding the use of public e-ID schemes (under the eIDAS Regulation) by the private sector, including financial services firms. Subject to any relevant constraints, there could be merit in facilitating the development of digital on-boarding processes, which build on the eIDAS Regulation. Another possibility would be for public authorities to cooperate with private sector digital identity solution providers and with PSPs on the development of national e-ID and eSignature solutions and connecting them to the eIDAS node.

Which data, where appropriate and in accordance with data protection rules, should be part of such a Digital Financial Identity, in addition to the data already required in the context of the anti-money laundering measures (e.g. data for suitability test for investment services; data for creditworthiness assessment; other data)?

As mentioned above, the LEI code is a necessary component of such DFIs. The European Systemic Risk Board set up a Task Force to make recommendations on greater adoption of LEI across the EU, one of which was to introduce legislation requiring all legal entities to have an LEI and that its LEI is also mandatory for financial transaction and public reporting.

Please explain your reasoning and also provide examples for each case you would find relevant.

N/A.

Question 19. Would a further increased mandatory use of identifiers such as Legal Entity Identifier (LEI), Unique Transaction Identifier (UTI) and Unique Product Identifier (UPI) facilitate digital and/or automated processes in financial services?

Yes.

[12] https://www.gleif.org/en/about/governance/annual-report

If yes, in which framework(s) is there the biggest potential for efficiency gains?

In any framework pertaining to regulatory, supervisory or public reporting.

The LEI is a 20-digit, alpha-numeric code that enables clear and unique identification of legal entities participating in financial transactions. The code is linked to a set of key reference information relating to the legal entity in question e.g. name and address.[13] Once a legal entity obtains a LEI code, the code is assigned to that legal entity for its entire life.

The LEI provides a unique identifier for all entities participating in financial transactions that can also be used on a cross border basis, through a free and open database updated on a daily basis. This common framework is crucial to identifying clearly each exposure for risk management of financial transactions, to create transparency, and conduct market surveillance. The use of the LEI also generates tangible benefits for businesses including simplified regulatory reporting; database management free of charges; more accurate calculation of counterparty exposures; improved risk management; and increased operational efficiencies. In this context, the LEI will provide benefits in terms of costs and new business opportunities, as a reliable, open, standardised, and high-quality legal entity reference data shared across the marketplace.[14]

Furthermore, to date the LEI code has proven to be a highly efficient and reliable means of identification for a broad variety of market participants and is currently prescribed under the following sectoral legislation:

- European Markets Infrastructure Regulation (EMIR) – counterparties to derivatives contracts as well as beneficiaries, brokers, CCPs and clearing members;
- Market Abuse Regulation (MAR) – issuers of financial instruments; entities involved or reporting in suspicious transactions;
- Capital Requirements Regulation (CRR) – credit and financial institutions;
- Alternative Investment Funds Directive (AIFMD) –funds and fund managers;
- Credit Rating Agencies Regulation (CRAR) – credit rating agencies and rated entities;
- Solvency II – pension funds and insurance companies;
- Central Securities Depositories Regulation (CSDR) – CSDs, CSDs' participants;
- Transparency Directive – issuers of financial instruments listed on Regulated Markets;

[13] The complete list is available at: https://www.gleif.org/en/about-lei/common-data-file-format
[14] Our Vision: One Identity Behind Every Business https://www.gleif.org/en/about/our-vision

- Prospectus Regulation – issuers of securities offered to the public or admitted to trading on a regulated market situated or operating within an EU member state;

- Markets in Financial Instruments Directive II (MiFID II)/ Markets in Financial Instruments Regulation (MiFIR) – clients of EU investment firms and trading venues that are legal persons;

- Securitisation regulation – reporting entities.

In the future, the broad category of identifiers (including LEI) may also play a relevant role in the supervision of security token offerings and in the development of possible trading solutions through DLT.

Question 20. In your opinion (and where applicable, based on your experience), what is the main benefit of a supervisor implementing (a) an innovation hub or (b) a regulatory sandbox as defined above?

ESMA's position on the benefits of implementing an innovation hub or a regulatory sandbox is developed in the joint ESAs Report on Regulatory Sandboxes and Innovation Hubs. ESMA reaffirms the conclusions of the Report and supports the prominent role innovation facilitators play in promoting cooperation and fostering the scaling up of innovation.

In general, innovation facilitators seek to promote innovation while ensuring that the regulatory framework applies regardless of the technology through which an activity is carried out. Meeting these aims together may require a delicate balance. Against this general background, innovation facilitators at national level are designed and implemented in line with the particular mandates given to NCAs.

Recognising the benefits of innovation facilitators, almost all Member States have established an innovation hub as of now. The number of regulatory sandboxes is meant to grow, from five currently operating in Denmark, Lithuania, Netherlands, Norway, Poland, to a few more as Austria, Greece, Italy, Slovakia, and Spain are considering and/or taking steps to implement such frameworks in their jurisdictions. This trend demonstrates that as innovation hubs and regulatory sandboxes have proved their merits, more member states have established hubs or progressed from hubs to testing in sandboxes.

ESMA also recognises that there are limitations and challenges with regards to the scaling of financial innovations across the EU that may not be solved through the activities of a network. If the barriers stem from variations in national regulatory requirements, then they cannot be solved via innovation facilitators or their coordination but instead need to be addressed by legislative means at the national level.

Since the joint ESAs Report on the topic, the concept of an innovation hub has developed and now includes (inter alia) support and advisory services, access to investor networks and accelerators. Given this development, it is now possible to distinguish between an innovation

hub and innovation office. An innovation hub is more extensive than an innovation office. It goes beyond the provision of non-binding guidance on the conformity of innovative financial products, financial services or business models with licensing or registration requirements and regulatory and supervisory expectations. Continual monitoring of developments in this area is needed and further analysis and definitional work may be merited in future.

Question 21. In your opinion, how could the relevant EU authorities enhance coordination among different schemes [innovation hubs and regulatory sandboxes] in the EU? Please rate each proposal from 1 to 5.

Key: 1 – irrelevant. 2 – rather not relevant. 3 – neutral. 4 – rather relevant. 5 – fully relevant.

Promote convergence among national authorities in setting up innovation hubs and sandboxes, through additional best practices or guidelines	5
Facilitate the possibility for firms to test new products and activities for marketing in several Member States ("cross border testing")	4
Raise awareness among industry stakeholders	5
Ensure closer coordination with authorities beyond the financial sector (e.g. data and consumer protection authorities)	5
Promote the establishment of innovation hubs or sandboxes with a specific focus (e.g. a specific technology like Blockchain or a specific purposes like sustainable finance)	3
Other	N/A

Please specify how else could the relevant EU authorities enhance coordination among different schemes in the EU.

ESMA's view is that the innovation hubs or sandboxes with a specific focus, as envisaged among the options in the question, would need to be carried out at national level. Cross border testing can only be conducted through participation of those Member States that are offering sandbox solutions.

The use of common definitions and terminology where possible across authorities and at ESAs level may also promote coordination. For example, there may be benefits to common usage of terms such as non-binding advice and close dialogue, closer collaboration and fostering an ecosystem.

Question 21.1 If necessary, please explain your reasoning and also provide examples for each case you would find relevant.

N/A.

Question 24. In your opinion, what should be done at EU level to achieve improved financial education and literacy in the digital context. Please rate each proposal from 1 to 5.

Key: 1 – irrelevant. 2 – rather not relevant. 3 – neutral. 4 – rather relevant. 5 – fully relevant.

More affordable access at EU level to financial data: unlikely to improve financial education literacy, which requires more basic skills	3
Supervisor hubs focused on guiding consumers in the digital world	4
Pan-European campaigns/hubs on digitalisation	3
Collect best practices	4
Promote digital financial services	3
Rules related to financial education	4

Question 25. If you consider that initiatives aiming to enhance financial education and literacy are insufficient to protect consumers in the digital context, which additional measures would you recommend?

More affordable access at EU level to financial data seems unlikely to generate large improvements in financial education literacy, which requires basic skills rather than knowledge of detailed financial data. However, enabling consumers to explore datasets may improve their knowledge directly. In addition, greater access may promote the development of third-party visualisation tools, raising awareness and knowledge.

Promoting digital financial services may help some consumers, but not all are comfortable with online tools, so there could be a risk of ‘crowding out’.

Section III: Promote a well-regulated data-driven financial sector

Question 26. In the recent communication "A European strategy for data", the Commission is proposing measures aiming to make more data available for use in the economy and society, while keeping those who generate the data in control. According to you, and in addition to the issues addressed in questions 27 to 46 below, do you see other measures needed to promote a well-regulated data driven financial sector in the EU and to further develop a common data driven financial sector in the EU and to further develop a common European data space for finance?

One issue relevant to a well-regulated data driven financial sector is regulatory scope around the various entities that transmit and facilitate access to data generated by others. These entities have become integral to the financial markets ecosystem and can play a key role in data access for the public. At present however, they are largely outside the scope of regulation. The EC could consider this situation in the context of its broader data strategy, including the need to evaluate and define the scope of various entities that could/should be brought within the regulatory remit.

Question 27. Considering the potential that the use of publicly available data brings in finance, in which areas would you see the need to facilitate integrated access to these data in the EU?

Establishment of a consolidated tape (CT) providing real-time information on transactions in equity instruments (OTC and on-venue) would mitigate the fragmentation of markets and allow market participants to have a reliable view of liquidity across the Union. It would also contribute to the development of a genuine single market for equity instruments in the EU and support the establishment of a capital markets union.

Our MiFID review report on the cost of market data and the equity CT recommended the establishment of a CT consolidating in real-time post-trade transparency information required under MiFIR for both on-venue and OTC-trades. Such a CT would enable market participants to access information on all transactions concluded in the EU, which is currently not possible. It would thereby contribute to a better market functioning and could be used to supplement best execution policies.

MiFID II provides the framework for establishing (multiple) CTP(s) for equity and non-equity instruments. Published post-trade information may be fragmented with respect to different financial instruments, trading venues and Approved Publication Arrangements. CTP(s) would by design mitigate such fragmentation.

Question 28. In your opinion, what would be needed to make these data easily usable across the EU?

Key requirements for efficient and easy use of data are standardisation, harmonisation, security of IT-systems and legal certainty regarding pertinent responsibilities, liabilities and usage permissions.

For publicly available data to be easily usable, they need to be subject to unrestricted access in a timely manner. Data standardisation is crucial (see answer to question 17), as is the need to address data quality issues through robust verification mechanisms.

All text data need to be in machine-readable format (.pdfs in particular do not count as machine readable). Institutions that produce .pdfs to satisfy their regulatory compliance needs should also be required to provide a text file that accompanies that .pdf.

Question 36. Do you/does your firm already deploy AI based services in a production environment in the EU? If yes, please specify for which applications.

ESMA has begun exploring new AI-based applications across the organisation. While still at a pre-production stage, activities under consideration include using text analysis (natural language processing methods) used to gauge market sentiment, and to reroute information more effectively across the organisation. In addition, an area of particular interest is also the potential for AI-based tools (such as machine learning) to support ESMA's statistics-related activities, such as for flagging outliers and inconsistent entries in the various databases that ESMA hosts.

Question 38. In your opinion, what are the most promising areas for AI- applications in the financial sector in the medium term and what are the main benefits that these AI-applications can bring in the financial sector to consumers and firms?

ESMA is aware of a number of case studies of financial sector firms and authorities developing AI tools to use in their work. Prominent examples include data management, market abuse and fraud detection (both from a RegTech and SupTech perspective) and (for firms) risk management.

Question 39. In your opinion, what are the main challenges or risks that the increased use of AI- based models is likely to raise for the financial industry, for customers/investors, for businesses and for the supervisory authorities? Please rate each proposal from 1 to 5.

1. **Financial industry**

Key: 1 – irrelevant. 2 – rather not relevant. 3 – neutral. 4 – rather relevant. 5 – fully relevant.

Lack of legal clarity on certain horizontal EU rules.	4
Lack of legal clarity on certain sector-specific EU rules	4
Lack of skills to develop such models	3
Lack of understanding from and oversight by the supervisory authorities	4
Concentration risks	2
Other	

Please specify what other main challenge(s) or risk(s) the increased use of AI- based models is likely to raise for the financial industry.

ESMA considers that the increased use of AI-based models would present a number of challenges for the financial industry. These include issues related to model explainability and possible bias, as well as model complexity, particularly where AI-based models are combined with other non-AI-based models that may be older.

From the perspective of skills shortages, this should be seen from a more detailed perspective. The deployment of AI-based models involves a number of different skills, with respect to:

- *constructing* AI-based models, for example with regard to certain input data selection and transformation choices (feature selection and pre-processing), modelling choices (specific AI model selected for the problem at hand, hyperparameter tuning, and model evaluation) and also data output choices (what data is produced, how it is meaningful)

- *maintaining* AI-based models once they are built, for example how to incorporate new or updated high-quality data into the models, and how often (and how much) to recalibrate them over time,

- *exploiting* AI-based models, for example how to store, disseminate, and embed insights from these models across the organisation, and

- *explaining* these models, for example to customers, other business lines within the organisation, and also to supervisory authorities.

It is important to note that each of these stages above are likely to require different skill sets, and that this will become more evident as the prevalence of AI-based models grows throughout the financial services industry. (Developing and acquiring appropriate skills is relevant not only to firms but also to supervisors and regulatory authorities.)

Managing risks associated with AI-based models is highly linked with having the necessary and appropriate skillsets above—these can almost be seen as a necessary condition to limit any follow-on risks stemming from the increasing use of these models throughout the financial services industry. For example, if traders or asset managers rely on the outputs of models without an appropriate level of understanding of how the outputs are generated, this could lead to a mispricing of risk and/or unpredictable feedback loops among trading strategies. These developments could in turn have a negative impact on market stability and order.

2. Consumers/investors

Key: 1 – irrelevant. 2 – rather not relevant. 3 – neutral. 4 – rather relevant. 5 – fully relevant.

Lack of awareness on the use of an algorithm	4
Lack of transparency on how the outcome has been produced	4
Lack of understanding on how the outcome has been produced	3
Difficult to challenge a specific outcome	4
Biases and/or exploitative profiling	4
Financial exclusion	3
Algorithm-based behavioural manipulation (e.g. collusion & other coordinated firm behaviour)	4
Loss of privacy	4
Other	

Please specify what other main challenge(s) or risk(s) the increased use of AI- based models is likely to raise for customers/investors.

AI-based models can be effective, and lead to increased speed and scale for financial services providers. However, as with all models, they make choices about information that is received, by separating this into idiosyncratic items that can safely be ignored and more meaningful information to which 'attention' must be paid to ('noise' vs. 'signal'). As with all models, AI-based models can get the balance between 'noise' and 'signal' wrong, for a variety of reasons that are either deep-seated (incorrect model) or temporary (model parameters need to be re-calibrated).

Following on from the above, consumers are presented with a unique set of risks with respect to AI-based models. The choices made about them can be driven by inappropriate modelling assumptions, i.e. an inappropriate balance placed on 'signal' vs. 'noise'. This is similar to a human employee misinterpreting the importance of information being provided by a client. However, whereas with an employee a customer can often see what went wrong—or at least request further information—it is often more challenging to do the same when an abstract model has made such a decision (and to judge how the model needs to be adjusted).

For this reason, it is important that customers are able to know when an algorithm has been used, as well as obtain transparency on the outcome. It seems less important (though still relevant) that consumers understand how this has been done, since they can also seek specialised advice on this (although lack of understanding can also lead to financial inclusion). It is also important for consumers to be legally empowered to challenge specific outcomes and seek redress—this empowerment is a straightforward way to limit the scope for AI-based models to be used to deliberately mislead consumers, in the same way that consumer law provides consumers with the ability to seek legal redress in the event of mis-selling.

3. Supervisory authorities

Key: 1 – irrelevant. 2 – rather not relevant. 3 – neutral. 4 – rather relevant. 5 – fully relevant.

Lack of expertise in understanding more complex AI-based models used by supervised entities	5
Lack of clarity in explainability requirements, which may lead to reject these models	3
Lack of coordination with other authorities (e.g. data protection)	3
Biases	4
Other	

Please specify what other main challenge(s) or risk(s) the increased use of AI- based models is likely to raise for the supervisory authorities.

Please see above with respect to sub-point 1 regarding skills and expertise. It is noted that the above skills considerations also apply to designing effective policy and supervisory requirements—without an expert-level understanding of the subject, it is also unlikely that effective, proportionate, and clear legislation and supervisory requirements can be developed.

Another aspect that may become more relevant is the provision of AI solutions by third parties. Smaller firms may not be in a position to develop solutions in-house, while larger firms may have specialised AI-units that serve a horizontal function spanning several risk categories.

Question 40. In your opinion, what are the best ways to address these new issues? Please rate each proposal from 1 to 5.

Key: 1 – irrelevant. 2 – rather not relevant. 3 – neutral. 4 – rather relevant. 5 – fully relevant.

New EU rules on AI at horizontal level	4
New EU rules on AI for the financial sector	2
Guidance at EU level for the financial sector	4
Experimentation on specific AI applications under the control of competent authorities	4
Certification of AI systems	4
Auditing of AI systems	4
Registration with and access to AI systems for relevant supervisory authorities	4
Other	

Please specify what other way(s) could be best to address these new issues.

With respect to the above table, it is noted that the recent expansion in AI-based models are not limited to the financial services sector and are instead likely to touch on many aspects of society. In addition, the potential and risks of AI-based models are not necessarily sector-specific. The fact that financial stability issues arise more in the context of financial services speaks more about limiting the consequences of these models' risks, but not about a sector-specific approach to legislation on the pure AI-specific risks of these models.

Nevertheless, guidance for the EU financial sector could still be welcome, as a complement to horizonal-level EU rules on AI.

It is also necessary to incorporate privacy considerations into any horizontal-level rules. Doing so would, almost inevitably, lead to a need to review other regulations, such as assessing whether the GDPR needs to be modified, strengthened, and/or clarified in certain respects.

Question 41. In your opinion, what are the main barriers for new RegTech solutions to scale up in the Single Market? Please specify what are the other main barrier(s) for new financial service providers solutions to scale up in the Single Market.

RegTech solutions can only be deployed extensively if there is regulatory certainty that these solutions are, in fact, complying with applicable regulation(s). Once this certainty is established, the returns to scale for market participants to develop these solutions should

provide adequate economic incentive for them to be rolled out. In addition, further harmonisation of EU rules would make the transition faster and more effective.

Question 42. In your opinion, are initiatives needed at EU level to support the deployment of these solutions, ensure convergence among different authorities and enable RegTech to scale up in the Single Market?

Yes.

Question 42.1 Please explain your answer to question 42 and, if necessary, please explain your reasoning and provide examples.

The answer to question 41 provides details. Providing certainty for RegTech solutions requires a fundamental re-consideration about how the EU can provide regulatory certainty to market participants. Such certainty (or near-certainty) is best provided at the EU level, rather than at the national level, given the need to support cross-border financial arrangements, also bearing in mind the Capital Markets Union.

Additionally, ESMA continues to coordinate the work of NCAs to share information on RegTech developments, for example in its Financial Innovation Standing Committee. With the other ESAs, ESMA also plays a role in coordinating at EU level within the Joint Committee and related forums such as EFIF. Information-sharing of specific cases may then point to further work involving ESMA, for example within its supervisory convergence remit.

Other possible initiatives at EU level in future that could support these solutions include information exchange regarding best practices on data-driven supervision and cooperation to develop relevant supervisory tools where possible.

Question 43. In your opinion, which parts of financial services legislation would benefit the most from being translated into machine-executable form? Please specify what are the potential benefits and risks associated with machine-executable financial services legislation.

It may make sense to think of a ‘cost plus complexity’ matrix when considering which parts of financial services legislation should be translated first. Those areas of (EU) legislation that carry the largest compliance costs for the (EU) financial services sector overall and which also have the highest degree of complexity (in terms of understanding, lack of harmonisation, etc.) would appear to be high priority for translation.

Notably, as RegTech solutions aim to provide clarity and certainty, they require a view of a given regulatory provision with reduced or minimal ambiguity. Machine-executable translation activity in and of itself can provide certainty to market participants.

A specific development to note in this area is that of security tokens, which use DLT as a basis. The first generation of security token platforms includes protocols aimed at automating certain regulatory compliance procedures such as those involving Anti Money Laundering and Know Your Customer requirements.

Question 44. The Commission is working on standardising concept definitions and reporting obligations across the whole EU financial services legislation. Do you see additional initiatives that it should take to support a move towards a fully digitalised supervisory approach in the area of financial services? Please explain your reasoning and provide examples if needed.

ESMA strongly supports these activities and stands ready to contribute where useful, including on the many pieces of delegated acts that ESMA has provided in draft form to the Commission over the years.

One example is ESMA's response to the 2017 Commission consultation document "Fitness Check on Supervisory Reporting", which highlighted the need for standardised definitions and reporting obligations.

This area touches also on two related topics: first, the need for centralization of public (and possibly supervisory) information, according to the model of repositories (such as securitisation repositories as per the Securitisation Regulation, or trade repositories as per the European Market Infrastructure Regulation and the Securities Financing Transactions Regulation).[15] The second relates to providing greater clarity in legislation regarding the terms 'machine-readable' and 'electronic format'—documentation that is in .pdf format for example is challenging to obtain information from, in contrast to more flexible formats that are used by issuers before conversion to .pdf.

One area in which ESMA has worked in recent years to foster digitisation and standardisation is the European Single Electronic Format (ESEF), the single electronic reporting format in which issuers on EU regulated markets are required to prepare their annual financial reports for financial periods beginning on or after 1 January 2020. The objectives of this project are to make reporting easier for issuers and to facilitate accessibility, analysis and comparability of annual financial reports, in particular by mandating the use of inline XBRL for marking-up ("tagging") IFRS consolidated financial statements. The ESEF relies on standardised definitions of accounting concepts provided by the IFRS taxonomy, which is prepared and annually updated by the IFRS Foundation through a rigorous due process. ESMA has drafted RTS which were adopted by the Commission as Delegated Regulation 2019/815 and in addition prepared guidance material. ESMA thinks that the ESEF has the potential to bring substantial benefits for issuers, investors and accounting enforcers. It could constitute the

[15] Regulations 2017/2402, 648/2012, and 2015/2365.

building block of further digitisation of reporting by companies, as indicated (among others) in ESMA's response to the EC consultation of revision of the Non-financial Reporting Directive.

Another area that would benefit from further standardisation and digitisation is that of Key Information Documents (KIDs), which are required to be produced for Packaged Retail and Insurance-Based Investment Products (PRIIPs). KIDs are publicly available, and the market size is worth an estimated several hundred billion euros, with an estimated hundreds of thousands of documents in circulation. However, there is no requirement for this information to be centralised, and PRIIPs KIDs, where available, are in .pdf formats and thus require intense effort to extract information from. This reality implies a challenge for monitoring this market segment (in line with investor protection mandates) as well as supervising it (in line with legislative mandates).

Question 45. What are the potential benefits and drawbacks of a stronger use of supervisory data combined with other publicly available data (e.g. social media data for effective supervision? Please explain your reasoning and provide examples if needed.

Using a risk-based approach to supervision is key to ensure that supervisory efforts and resources are employed where they are needed the most and where they can and should have the highest impact. This approach allows targeting supervisory intervention on the relevant risks and problems and on the basis of a clear understanding of the risk / problem in question, in order to focus on the actual cause(s) rather than on symptoms or ancillary issues.

In this context, employing a data-driven approach to supervision allows a thorough understanding of the supervised landscape, specific issues and risks/ problems. A clear analysis and understanding of the data available will support the entire supervisory framework, from identifying, assessing and prioritising risks and problems, to targeting the supervisory monitoring and intervention, to assessing the impact of supervisory effect and identifying lessons for the future.

At the same time, this stronger use of data needs to be matched with a corresponding adjustment in resources (mainly in terms of staff and technical tools). Drawbacks may arise in the absence of a risk-based supervisory model that enables the correct processing of the concerns identified through the data. Another important challenge is the need to verify data quality and accuracy through robust mechanisms. In particular, social media data, to the extent used, may often be of low quality.