EUROPEAN
COMMISSION

Brussels, 8.3.2018
COM(2018) 109 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN CENTRAL BANK, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

FinTech Action plan: For a more competitive and innovative European financial sector

INTRODUCTION

FinTech — technology-enabled innovation in financial services — has developed significantly over recent years and is impacting the way financial services are produced and delivered. FinTech[1] sits at the crossroads of financial services and the digital single market. The financial sector is the largest user of digital technologies and represents a major driver in the digital transformation of the economy and society. There are important synergies between the Commission's Digital Single Market Strategy[2], the EU's cybersecurity strategy[3], the eIDAS Regulation[4] and financial services initiatives such as the Consumer Financial Services Action Plan[5] and the Capital Markets Union (CMU) mid-term Review[6].

While innovation in finance is not new, investment in technology and the pace of innovation have increased considerably. FinTech solutions using digital identification, mobile applications, cloud computing, big data analytics, artificial intelligence, blockchain and distributed ledger technologies are being rolled out. New technologies are changing the financial industry and the way consumers and firms access services, creating opportunities for FinTech-based solutions to provide better access to finance and to improve financial inclusion for digitally connected citizens. It places customers in the driving seat, supports operational efficiency and increases further the competitiveness of the EU economy. FinTech is also important for the Capital Markets Union. It can help to deepen and broaden EU capital markets by integrating digitisation to change business models through data-driven solutions for example in asset management, investment intermediation and product distribution[7].

FinTech also presents opportunities and challenges for regulatory compliance and supervision. It can facilitate, streamline and automate compliance and reporting and improve supervision. Service providers may offer FinTech-based compliance services to regulated entities. Regulated entities themselves remain, however, responsible for meeting their obligations. For example entities subject to customer due diligence requirements under anti-money laundering regulation can not delegate responsibility for meeting these requirements to external service providers.

FinTech also presents challenges such as cyber-related risks, data, consumer and investor protection issues and market integrity issues. The General Data Protection Regulation and the Anti-Money Laundering Directive provide fundamental safeguards for the protection of personal data and the integrity of the EU financial system against money laundering and terrorism finance. A technology enabled EU financial market place requires full compliance with these fundamental safeguards. Cyber risks undermine confidence and represent a threat

[1] FinTech is a term used to describe technology-enabled innovation in financial services that could result in new business models, applications, processes or products and could have an associated material effect on financial markets and institutions and how financial services are provided. See http://www.fsb.org/what-we-do/policy-development/additional-policy-areas/monitoring-of-FinTech/.
[2] COM(2015) 192 final — A Digital Single Market Strategy for Europe.
[3] JOIN/2017/0450 final — Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.
[4] Regulation (EU) No 910/2014 of The European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[5] COM/2017/0139 final — Consumer Financial Services Action Plan: Better Products, More Choice.
[6] COM(2017) 292 final — Communication on the Mid-Term Review of the Capital Markets Union Action Plan.
[7] Mid-Term Review of the Capital Markets Union, available here.

to the stability of the financial system. Regular security breaches[8] underscore that cyber-attacks are a growing concern. Such attacks should be tackled in a decisive way to prevent and mitigate any negative consequences for the financial sector, its clients and its customers. Making the financial sector more cyber resilient is of paramount importance to ensure that it is well protected, that financial services are delivered effectively and smoothly across the EU, and that consumer and market trust and confidence are preserved.

Europe's regulatory and supervisory frameworks should allow firms operating in the EU Single Market to benefit from financial innovation and provide their customers with the most suitable and accessible products. Such frameworks should also ensure a high level of protection for consumers and investors and ensure the resilience and integrity of the financial system. The benefits of technological innovation were already at the heart of the revisions to the Payment Services Directive[9] and to the Directive and Regulation on Markets in Financial Instruments[10].

Technological innovation has led to new types of financial assets such as crypto-assets. Such crypto-assets and the underlying blockchain technology hold promise for financial markets and infrastructures. Their use also presents risks, as has been witnessed by strong volatility of crypto-assets, fraud and operational weaknesses and vulnerabilities at crypto-asset exchanges. At EU level, action has already been taken to address some specific risks. The threat and vulnerability of virtual currencies and money laundering and terrorist financing was assessed as significant to highly significant in the Commission's Report on the assessment of the risks of money laundering and terrorist financing.[11] In December 2017, European legislators agreed to extend the scope of the Anti-Money Laundering Directive[12] to virtual currency exchanges and wallet providers. The European Supervisory Authorities (ESAs) issued warnings about the speculative market environment for virtual currencies and other risks associated with crypto-assets.[13] All warnings point to the fact that crypto-asset investment is high risk and that investors may incur substantial losses due to their volatility but also due to the lack of market

[8] In 2016, the financial sector was targeted by cyber-attacks 65 % more often than any other sector. This resulted in more than 200 million records being breached, a 937 % increase over 2015 when just under 20 million were breached. Source: IBM 'Security trends in the financial services sector', April 2017.

[9] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

[10] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and Regulation EU 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.

[11] Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. COM(2017)340 final, 26.6.2017

[12] Directive (EU) 2015/849 of the European Parliamet and of the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing.

[13] Warning to consumers on Virtual Currencies. EBA/WRG/2013/01 - https://eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf; EBA Opinion on Virtual Currencies – EBA/Op/2014/08 - https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf; ESMA alerts investors to the high risks of Initial Coin Offerings – ESMA50-157-829 - https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf; ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements – ESMA50-157-828 - https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf; ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies – 12 February 2018 - https://www.eba.europa.eu/documents/10180/2120596/Joint+ESAs+Warning+on+Virtual+Currencies.pdf

transparency and integrity and operational weaknesses as well as vulnerabilities in crypto-asset services and trading venues.

In its recent initiative to review the European supervisory framework[14], the Commission proposed that the European Supervisory Authorities should systematically consider FinTech in all their activities. The General Data Protection Regulation (GDPR), which will become applicable in May 2018, is also of critical importance for a proper use of innovative data-driven financial services[15] as is the proposal for a Regulation on a framework for the free flow of non-personal data in the EU[16], which seeks to ensure that non-personal data can move freely across the single market. Additionally, the cross border recognition of electronic means of identification provided by the eIDAS Regulation will provide safeguards and mitigate risks from emerging technologies, while making it easier to meet customer due diligence anti-money laundering requirements and strong authentication of parties in a digital environment.

FinTech is a priority area also at the international level, for example for the G20. The Commission contributes to policy discussions at the Financial Stability Board and in other international fora. An increasing number of jurisdictions have developed regulatory and supervisory frameworks to address specific forms of FinTech innovation. Outside Europe, regulators have mainly focused on payment instruments and services and alternative forms of financing, such as crowdfunding and peer-to-peer lending. For more interaction with FinTech developers, a number of supervisors (e.g. Australia, Canada, the United States, Hong Kong, Singapore and Japan) have set up FinTech hubs. Several authorities have also developed experimentation frameworks for innovative firms called 'regulatory sandboxes' (e.g. Australia, Hong Kong, Singapore and Canada).

The Commission aims to respond to the calls by both the European Parliament[17] and the European Council[18] for a more future-oriented regulatory framework embracing digitalisation and creating an environment where innovative FinTech products and solutions can be rapidly rolled out across the EU to benefit from the economies of scale of the single market, without compromising financial stability or consumer and investor protection.

Drawing on the conclusions from the public consultation[19] in March-June 2017 and taking account of the initiatives already presented, the Commission considers that the case for broad legislative or regulatory action or reform at EU level at this stage is limited. A number of

[14] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/european-system-financial-supervision_en#reviewoftheesfs .

[15] The GDPR creates a genuine single market for the free movement of personal data at a high level of personal data protection. FinTech shall be fully compliant with applicable personal data protection rules.

[16] Com(2017)495.

[17] The European Parliament has called on the Commission 'to deploy a proportionate, cross-sectorial and holistic approach to its work on FinTech' — 'Report on FinTech: the influence of technology on the future of the financial sector', Committee on Economic and Monetary Affairs, Rapporteur: Cora van Nieuwenhuizen, 2016/2243(INI), 28 April 2017.

[18] EUCO 14/17, CO EUR 17, CONCL 5 see http://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf
The European Council 'calls on the European Commission to put forward the necessary initiatives for strengthening the framework conditions with a view to enable the EU to explore new markets through risk-based radical innovations and to reaffirm the leading role of its industry', 19 October 2017.

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

targeted initiatives for the EU to embrace digitalisation of the financial sector are, however, warranted.

1. ENABLING INNOVATIVE BUSINESS MODELS TO REACH EU SCALE

1.1. Enabling innovative business models to scale-up across the EU through clear and consistent licensing requirements

In the financial sector, firms are authorised and supervised based on their activities, services or products, regardless of whether they use traditional or innovative means to deliver those services. Depending on the services and products offered, firms can be authorised and regulated under EU or national law, or not be subject to any financial services specific regulation.

Authorisation requirements allow for effective supervision of service providers to ensure the stability, integrity, and fairness of markets. They also ensure that consumers and investors are protected. At the same time, uniform operating conditions enable EU financial services firms that are duly authorised and supervised by their home Member State to benefit from a European passport. This passport gives these firms the possibility to provide their services in all other Member States and to scale up in the entire EU Single Market.

Respondents to the FinTech consultation considered that most innovative business models could work under existing EU rules, given that the EU legislative framework provides room to apply proportionality in the authorisation process.

Yet supervisors may take different approaches to identifying the applicable EU legislative framework and applying proportionality when licensing innovative business models[20]. The European Banking Authority identified differences in authorisation and registration regimes[21] as an area requiring further attention. EIOPA observed similar trends[22]. The European Central Bank (ECB) also recently launched a consultation on a 'Guide to assessments of FinTech credit institution license applications'[23].

New financial services do not always fall fully under the existing EU regulatory framework; this is the case of crowd and peer-to-peer activities for start-ups and scale-up companies. A large number of respondents to the FinTech consultation highlighted that investment-based and lending or loan-based crowdfunding activities would benefit from a sound and proportionate EU regulatory framework. 11 Member States have already adopted bespoke regimes which are often conflicting and hampering the development of a Single Market for crowdfunding services. A lack of a common EU framework also hinders the ability of crowdfunding providers to scale-up within the Single Market mainly due to conflicting approaches to national supervision and regulation. The EU framework proposed in this Action Plan will offer a comprehensive European passporting regime for those market players who decide to operate as European crowdfunding service providers (ECSP). This framework will provide incentives for crowdfunding service providers to scale-up while ensuring sufficient protection for investors and project owners.

[20] Such as online platforms acting as brokers/intermediaries, p2p insurance, virtual currencies and automated investment advice, Initial Coin Offering, etc.

[21] https://www.eba.europa.eu/-/eba-publishes-a-discussion-paper-on-its-approach-to-FinTech.

[22] https://eiopa.europa.eu/Publications/Reports/Sixth%20Consumer%20Trends%20report.pdf

[23] https://www.bankingsupervision.europa.eu/press/pr/date/2017/html/ssm.pr170921.en.html.

Further efforts are needed to identify diverging licensing requirements that affect FinTech firms. Follow-up actions could include:

- clarifying the applicable EU legislative framework for services;
- assessing the need for an EU framework to cover new innovative business models; and
- providing guidance to national supervisors to ensure more convergence between national regulatory regimes.

Moreover, supervisors have been assessing market developments in crypto-assets and the emergence of initial coin offerings (ICOs), a new way of raising money using what are called 'coins' or 'tokens'. While such token sales may offer firms new and innovative ways of raising capital, they can also present clear risks to investors. Speculative investments in crypto-assets and ICO-tokens expose investors to significant market risk, fraud and to cybersecurity risks arising from exchanges and service providers that allow investors to purchase crypto assets and tokens, hold them or trade them. In November 2017, the European Supervisory Markets Authority (ESMA) issued two statements[24] to inform investors of potential risks posed by certain ICOs and to remind firms involved in ICOs that these activities may fall under existing EU legislation, depending on their precise structure and characteristics. Authorities in the EU and across the world are evaluating ICOs and regulation that may be applicable to them, while China and South Korea have banned them.

The rapid price increase and volatility of crypto-assets over the past months requires a better understanding of the risks and opportunities that go with their use and a better understanding of the applicability of EU regulation. However, crypto-assets and tokens may also escape regulation and the transparency, governance and investor protection objectives regulation pursues. In February 2018, following a request by the European Commission, the three European Supervisory Authorities (ESAs) published a joint warning to investors and users on the risks associated with buying crypto-assets.[25] Also the changes to the 4th Anti-Money Laundering Directive on which the European Parliament and the Council reached an agreement in December 2017 will reduce anonymity and increase the traceability of transactions by requiring crypto-asset exchanges and custodial wallet providers in the European Union to carry out customer identification and to exercise due diligence.

An assessment of the suitability of the current EU regulatory framework with regard to Initial Coin Offerings and crypto-assets more generally is necessary. On the one hand, the aim should be to make sure, that EU firms, investors and consumers can take advantage of this technical innovation within a fair and transparent framework in order to make Europe a leading player in developing new ways to rapidly fund growing businesses. On the other hand, potential financial stability, market integrity, investor and consumer protection, personal data protection and money laundering and terrorist financing-related risks should be appropriately addressed. As crypto-assets are a worldwide phenomenon, international coordination and consistency, for example within the G20, the Financial Stability Board (FSB) and international financial standard setters, will be essential. The Commission will

[24] https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms, 13 November 2017

[25] ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies – 12 February 2018 - https://www.eba.europa.eu/documents/10180/2120596/Joint+ESAs+Warning+on+Virtual+Currencies.pdf

work with supervisors, regulators, industry and civil society, both within the EU and with partners internationally, to determine any further appropriate course of action.

Box 1

1. **Together with this Communication, the Commission is presenting a proposal for an EU Regulation on investment-based and lending-based crowdfunding service providers (ECSP) for business. The proposal aims to ensure an appropriate and proportionate regulatory framework that allows crowdfunding platforms that want to operate cross-border to do so with a comprehensive passporting regime under unified supervision.**

2. **The Commission invites the European Supervisory Authorities, by Q1 2019, to map current authorising and licensing approaches for innovative FinTech business models. In particular, they should explore how proportionality and flexibility in the financial services legislation are applied by national authorities. Where appropriate, the ESAs should issue guidelines on approaches and procedures or present recommendations to the Commission on the need to adapt EU financial services legislation.**

3. **In the course of 2018, the Commission will continue monitoring the developments of crypto-assets and Initial Coin Offerings with the ESAs, the European Central Bank and the FSB as well as other international standard setters. Based on the assessment of risks, opportunities and the suitability of the applicable regulatory framework, the Commission will assess whether regulatory action at EU level is required.**

1.2. Increasing competition and cooperation between market players through common standards and interoperable solutions

The production and delivery of financial services requires different operators in the value chain to cooperate and interact. An EU-wide FinTech market will not reach its full potential without the development of open standards that increase competition, enhance interoperability and simplify the exchange of and access to data between market players.

There are different ways to implement interoperability. Companies or technology providers may develop *ad hoc* interfaces to which other parties need to adapt. Another approach is to reach consensus on interoperability standards for the whole market, reducing the efforts required for service providers to exchange data with different platforms. Standard-setting processes should be based on the principles of openness, transparency and consensus, in accordance with Regulation (EU) No 1025/2012 on European standardisation. For standards to be pro-competitive, participation should be unrestricted and the procedure for adopting the standard should be transparent, allowing stakeholders to effectively inform themselves of standardisation work. Effective access to the standard should be provided on fair, reasonable and non-discriminatory terms.

Most respondents to the FinTech consultation stressed that it is a priority to develop standards, promote their adoption, and ensure interoperability between systems. The preferred approach would be led by industry and market participants, developing global standards as opposed to local or regional standards. There is particular demand for greater standardisation

in blockchain/distributed ledger technologies, application programming interfaces and identity management. The revised Payment Services Directive, in application since January 2018, is an interesting test case: banks are required to open appropriate communication channels for FinTechs to provide their services based on access to payment accounts. The development of standardised application programming interfaces would create a level playing field to enable new and improved services in a truly open environment, while maintaining high standards of protection of personal data and consumer protection.

Box 2

1. **The Commission will help to develop more coordinated approaches on standards for FinTech by Q4 2018 by liaising and working with major standard-setting bodies, such as European Committee for Standardisation and International Organisation for Standardisation including in the blockchain area.**

2. **The Commission encourages and will support joint efforts by market players to develop, by mid-2019, standardised application programming interfaces that are compliant with the Payment Services Directive and the General Data Protection Regulation as a basis for a European open banking eco-system covering payment and other accounts.**

1.3. Facilitating the emergence of innovative business models across the EU through innovation facilitators

Innovative companies bring new products to the market or provide ways to provide well-known services in innovative forms or at more competitive prices. Innovators need to be able to extend their services to as wide a base of users as possible, leveraging economies of scale. In order to fully benefit from the single market, innovators should be able to use a European passport. This requires meeting regulatory requirements that may be difficult to fulfil. This is particularly the case for newly established businesses and for those employing innovative technologies or models that may differ from standard practices in place at the time rules were adopted.

Innovative approaches and technologies also challenge financial supervisors when deciding to authorise or not a firm or activity and determining how to fulfil their supervisory obligations. Responses to the Commission's public consultation suggest there is a strong appetite among supervisors to better understand the latest FinTech trends and to strengthen contacts with firms and other technology providers.

In the EU, 13 Member States have established what are called 'FinTech facilitators' (innovation hubs[26] or regulatory sandboxes[27]) to provide general guidance to firms during the

[26] See EBA/DP/2017/02 — 'Innovation hub' means an institutional arrangement where regulated or unregulated entities (i.e. unauthorised firms) engage with the competent authority to discuss FinTech-related issues (share information and views, etc.) and seek clarification on the conformity of business models with the regulatory framework or on regulatory/licensing requirements (i.e. individual guidance to a firm on the interpretation of applicable rules).

authorisation process. This enables such firms to gain quicker access to the market and better understand the rules and supervisory expectations. The facilitators may also provide guidance to established financial institutions. From the supervisors' perspective, such approaches provide an important source of information, helping them acquire a better understanding of innovative business models and market developments at an early stage.

Regulatory sandboxes take the idea of innovation hubs a step further by creating an environment where supervision is tailored to innovative firms or services. National competent authorities must apply relevant EU financial services legislation. However, these rules include a margin of discretion with regard to the application of the proportionality and flexibility principles embedded in these rules. This can be particularly useful in the context of technological innovation.

The sandbox approach by has been supported by industry respondents to the public consultation. National authorities expressed mixed views: some supervisors consider that such initiatives are not part of their mandate; supervisors that are open to sandboxes, by contrast, consider that others should take similar initiatives. A consistent approach among supervisors would foster the roll out innovation across the EU single market.

Recently, both EBA, EIOPA and ESMA mapped the existing innovation facilitators across the EU. The Commission would welcome further efforts to identify best practices across the EU and set up common principles and criteria for innovation hubs and regulatory sandboxes. Other follow-up actions could include promoting the setting-up of innovation hubs in all Member States and coordinating their operations. This could lead to considering an EU experimentation framework for adopting and adapting to new technologies.

Box 3

1. **Building on recent work by the ESAs to map FinTech facilitators set up by national supervisory authorities, the Commission invites the ESAs to conduct further analysis and identify best practices by Q4 2018 and, where appropriate, to issue guidelines on these facilitators.**

2. **The Commission invites competent authorities at Member State and EU level to take initiatives to facilitate innovation on the basis of these best practices and invites the ESAs to facilitate supervisory cooperation, including coordination and dissemination of information regarding the innovative technologies, establishment and operation of innovation hubs and regulatory sandboxes, and consistency of supervisory practices.**

3. **Based on the work of the ESAs, the Commission will present a report with best practices for regulatory sandboxes by Q1 2019.**

[27] See EBA/DP/2017/02 — Regulatory 'sandboxes' provide financial institutions and non-financial firms with a controlled space in which they can test innovative FinTech solutions with the support of an authority for a limited period of time, allowing them to validate and test their business model in a safe environment.

2. SUPPORTING THE UPTAKE OF TECHNOLOGICAL INNOVATION IN THE FINANCIAL SECTOR

2.1. Reviewing the suitability of our rules and ensure safeguards for new technologies in the financial sector

Technology neutrality is one of the guiding principles of the Commission's policies.

Nevertheless, EU rules that pre-date the emergence of innovative technologies may in practice not always be technology-neutral towards these innovations. Respondents to the public consultation have, for example, pointed to requirements or preferences for paper-based disclosures, or the need for physical presence. The absence of clear and harmonised processes to identify consumers and businesses online, in full compliance with anti-money laundering and data protection rules, was also considered a challenge for FinTech solutions. In the same vein, respondents expressed concerns that software investment is less attractive under current prudential rules for banks where investments in software made by EU banks must be deducted from their regulatory capital, in contrast to the more favourable treatment enjoyed by banks in the United States.

The Commission has already given consideration to some of these issues. In the Consumer Financial Services Action Plan[28], the Commission announced its intention to facilitate the cross-border acceptance of e-identification and remote know-your-customer processes. The aim is to enable banks to identify consumers digitally in compliance with anti-money laundering and data protection requirements, making full use of the electronic identification and authentication tools provided under eIDAS. To facilitate the use of electronic identification and authentication, the Commission set up[29] a dedicated expert group on electronic identification and remote know-your-customer processes. The uptake of disruptive technologies, such as distributed ledger technologies and artificial intelligence, may pose additional regulatory challenges. Requirements for paper-based disclosure should be addressed. Responses to the public consultation raise concerns that the use of such technologies may be prevented or constrained by the existing rules, for example in the following ways:

- blockchain-based applications may raise jurisdictional issues about the law applicable and liability issues;
- the legal validity and enforceability of smart contracts may need clarification;
- there are uncertainties surrounding the legal status of ICOs and the rules applicable to them, as set out already under point 1.1. above;

Further analysis is necessary to assess the extent to which the legal framework for financial services is technology neutral and able to accommodate FinTech innovation, or whether it needs to be adapted to this end. At the same time, it is necessary to ensure that financial stability, consumer and investor protection, anti-money laundering requirements and law enforcement are respected.

[28] COM(2017)139 final.
[29] Commission Decision C(2017)8405 of 14 December 2017.

Box 4

The Commission will set up an expert group to assess by Q2 2019 whether there are unjustified regulatory obstacles to financial innovation in the financial services regulatory framework.

2.2. Removing obstacles to cloud services

Cloud computing can increase the efficiency of the digital infrastructure which underpins financial services. Outsourcing data processing and storage capacity to cloud service providers reduces the cost of hosting, infrastructure and software for firms and can help streamline IT expenditure. At the same time, it can ensure greater performance, flexibility and adaptability.

Regulated firms that outsource activities to a cloud service provider must comply with all legal requirements (e.g. in terms of proper risks management, data protection and appropriate oversight by supervisors). Stakeholders responding to the Commission consultation raised concerns that uncertainties over financial supervisory authorities' expectations were limiting the use of cloud computing services. Such uncertainties are due in particular to the absence of harmonisation of national rules and different interpretations of outsourcing rules[30].

The EBA recently published recommendations on outsourcing to cloud services[31]. ESMA, in its role as direct supervisor for credit rating agencies and trade repositories, is exploring these issues and in 2018 intends to clarify which requirements these firms have to comply with when outsourcing to cloud services. Outsourcing to cloud services is also part of EIOPA's mandate in the InsurTech area. Nevertheless, the issue deserves attention beyond the scope of these existing initiatives. Additional certainty could be achieved if supervisory expectations were expressed in the form of formal guidelines of the ESAs.[32]

The Commission's proposal for a Regulation establishing a framework for the free flow of non-personal data in the EU aims to remove unjustified data localisation restrictions and thus tackle one of the main problems identified. The proposal also addresses additional cloud-related issues, such as preventing vendor lock-in by cloud service providers. To facilitate the implementation of the proposed Regulation specifically in relation to the use of cloud services, the Commission will in 2018 gather relevant stakeholders, consisting of cloud users, cloud providers and regulatory authorities.

[30] Respondents to the FinTech consultation proposed that standardised contractual agreements between cloud and financial service providers could better reflect their sectoral regulatory constraints (such as audit obligations, or requirements for onsite inspections). Data localisation restrictions by public authorities constituted another important obstacle identified by respondents. In the context of a highly concentrated market for cloud services, financial institutions and supervisors also raised the risk of high dependency on a handful of non-EU providers and the need to prevent European financial institutions from becoming locked-in with suppliers.

[31] EBA/REC/2017/03, *Recommendations on outsourcing to cloud service providers,* December 2017, available here.

[32] As regard requirements of the personal data protection legislation, the coordination of the approaches taken by Data Protection supervisorsis already regulated under GDPR.

Box 5

1. **The Commission invites the ESAs to explore the need for guidelines on outsourcing to cloud service providers by Q1 2019.**

2. **In the context of the Communication on Building the European Data Economy, the Commission invites cloud stakeholders to develop cross-sectoral self-regulatory codes of conduct to facilitate switching between cloud service providers. The Commission will also invite representatives from the financial sector to enable easier data porting also for financial institutions.**

3. **In this context, the Commission shall encourage and facilitate the development of standard contractual clauses for cloud outsourcing by financial institutions, building on the cross-sectorial cloud stakeholder efforts already facilitated by the Commission, and ensuring financial sector involvement to this process. This work should be undertaken by a balanced mix of companies from the financial sector and cloud service providers, and should address in particular audit requirements, reporting requirements or the determination of materiality of the activities to be outsourced.**

2.3. Enabling FinTech applications with the EU blockchain initiative

Blockchain and distributed ledger technologies will likely lead to a major breakthrough that will transform the way information or assets are exchanged, validated, shared and accessed through digital networks. They are likely to continue to develop in the coming years and become a key component of the digital economy and society.

It is important to avoid confusion between blockchain technologies and crypto-assets (mentioned above), which represent just one type of application of blockchain. Blockchain can underpin a wide range of applications in various sectors, which may not be limited to crypto-assets or even FinTech at all.

The financial sector has been leading the exploration of the potential of blockchain with many proofs of concept and pilot projects in a wide range of areas such as payments, securities, deposits and lending, capital raising, investment management, market provisioning, trading and post-Trade as well as trade finance and reporting (e.g. RegTech).

Distributed ledger technologies and blockchain have great potential to drive simplicity and efficiency through the establishment of new infrastructure and processes. These technologies may become central to future financial services infrastructure. The most impactful applications will require deep collaboration between incumbents, innovators and regulators to have a successful and beneficial implementation path. The scope of potential applications is very broad and should be monitored closely.

Even though blockchain technologies are still at an early stage, a number of challenges and risks need to be addressed.The EU Blockchain Observatory and Forum[33], which was launched in February 2018 for a period of 2 years, aims to monitor trends and developments, pooling expertise to address sectoral and cross-sectoral issues and exploring joint solutions and cross-border cases of blockchain use. The European Parliament also supported the launch of the European Financial Transparency Gateway (EFTG), a pilot project using distributed ledger technology to facilitate access to information about all listed companies on EU securities regulated markets in the context of the Transparency Directive[34]. This initiative aims to increase transparency of EU regulated markets, fostering both market integration and market liquidity, in line with the objectives of the capital markets union. The European Commission also initiated, for example, blockchain for industrial transformations (#Blockchain4EU) and the proof of concept to use blockchain to facilitate the collection of excise duties.

Considering the cross-cutting nature of blockchain, which goes beyond financial services and potentially encompasses all sectors of the economy and society, the Commission has already taken steps to set up an EU blockchain initiative with the launch of the EU Blockchain Observatory and Forum. The initiative will propose actions, funding measures and a framework to enable scalability, develop governance and standards, and to support interoperability. It is a cross-sectoral initiative expected to enable early adoption of this technology in the financial sector and increase Europe's competitiveness and technological leadership, in collaboration with other actions in this action plan (notably, the suitability check of EU financial legislation). It will rely also on pilot actions supported through the Horizon 2020 programme, which will be expanded during 2018-2020. The Commission has also developed links with the International Standards Organisation Technical Committee 307 on blockchain and distributed ledger technologies. European Standardisation Organisations[35] have been invited to take on a leadership role to identify specific EU features for blockchain.

Box 6

[33] https://ec.europa.eu/digital-single-market/en/news/pre-information-notice-eu-blockchain-observatory-forum.
[34] Directive 2013/50/EU.
[35] CEN, CENELEC and ETSI.

1. **The Commission will consult publicly on further digitisation of regulated information about companies listed on EU regulated markets in Q2 2018, including the possible implementation of a European Financial Transparency Gateway based on distributed ledger technology.**
2. **The Commission will continue to work on a comprehensive strategy, considering all relevant legal implications, on distributed ledger technology and blockchain addressing all sectors of the economy, including enabling FinTech and RegTech applications in the EU.**
3. **The Commission launched an EU Blockchain Observatory and Forum in February 2018, as well as a study on the feasibility of an EU public blockchain infrastructure to develop cross-border services. It will be assessed whether block chain can be deployed as a digital services infrastructure under the Connecting Europe Facility.With the support of the EU Observatory and Forum and the European Standardisation Organisations, the Commission will continue to appraise legal, governance and scalability issues and support interoperability and standardisation efforts, including further evaluating cases of blockchain use and its applications in the context of the Next Generation Internet.**

2.4. Building capability and knowledge among regulators and supervisors in an EU FinTech Lab

Major hurdles preventing the financial industry from taking up new technology include a lack of certainty and guidance on how to use it, fragmentation and a lack of common approaches between national regulators and supervisors.

Some technology providers already make efforts to inform regulators and supervisors about the nature of their technologies and how they are applied in the financial sector. However, many authorities are reluctant to receive training or engage in discussions when hosted by selected vendors.

The Commission will establish an EU FinTech Lab to raise the level of regulatory and supervisory capacity and knowledge about new technologies. It will do this through demonstrations and expert discussion in a non-commercial, neutral financial technology Laboratory. The Lab will bring together multiple vendors, in particular from the EU, with regulators and supervisors so they can raise and discuss regulatory and supervisory concerns.

The technologies addressed could include:

- authentication and identification technologies,
- specific cases for using distributed ledger technology, cloud technology, machine learning and artificial intelligence,
- application programming interfaces and open banking standards and
- RegTech.

Box 7

The Commission will host an EU FinTech Lab where European and national authorities will be invited to engage with technology solution providers in a neutral, non-commercial space during targeted sessions on specific innovations starting in Q2 2018.

2.5. Leveraging technology to support distribution of retail investment products across the Single Market

Today, retail investors engaging with capital markets are overwhelmed by the sheer complexity, the cost and the uncertainty associated with investment products. Significant progress has been made in improving the comparability of retail investment products notably through disclosure requirements. While this should improve the quality of products, retail investors still face substantial search costs in selecting the most suitable investment product.

Increased transparency to stimulate competition and widen the choices for retail investors in capital markets should therefore be underpinned by data-driven solutions that would use new, more effective technologies ensuring that information is complete, comparable and easily accessible. Such tools could be based on publicly available disclosures and provide a user-friendly interface linking existing databases or digital tools such as online calculators, comparison tools, automated-advisors or fund supermarkets. To this end, substantial work is needed for ensuring the interoperability of datasets and the development of appropriate algorithms, whilst making sure that results are presented in a fair and easy to understand way. The Commission will therefore examine the current landscape and situation of technology-driven digital interfaces that help individuals to find suitable and cost-effective retail investment products across the EU's capital markets.

3. ENHANCING SECURITY AND INTEGRITY OF THE FINANCIAL SECTOR

Cybersecurity remains at the centre of EU policy action and making the EU financial sector more cyber resilience is a policy priority for the Commission Nonetheless, high-profile cyber-attacks focus attention on the continued need to ensure the resilience and integrity of systems. The cross-border nature of cyber-threats requires a high degree of alignment of national regulatory and supervisory requirements and expectations. As the financial sector becomes increasingly dependent on digital technology, ensuring that the financial sector is safe and resilient is essential. In this respect, the Commission aknowledges the importance for digital services to incorporate a 'security by design approach' and, in this respect, has already put forward a proposal[36] to create an EU certification framework for ICT security products and services.

While the financial sector is better prepared than other sectors, it is also the sector most under attack. Operational and cyber risks pose a mounting threat to the stability of the financial system and undermine the confidence that is vital for our financial markets. Recognising the

[36] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

potential threat to the financial sector's stability, the European Parliament has called on the Commission 'to make cybersecurity the number one priority in the FinTech action plan'[37]. Repeated cyber incidents triggered by the exploitation of basic security flaws in systems and organisations underscore the critical importance of practising fundamental cyber hygiene[38] within any organisation. Stricter cyber hygiene measures and requirements is crucial to ensure integrity. However, the degree to which firms are subject to and strengthen their cyber hygiene standards varies across the EU, depending largely on industry and national practices. At EU level, current financial services legislation, in particular covering financial market infrastructures and payments, already contains specific requirements on the integrity of IT resources and systems and their governance. In other areas, requirements are more general, for example in the case of business continuity or general operational risk requirements.

The transposition by Member States of the directive on security of network and information systems[39] (NIS) provisions on security requirements in other financial services is on-going. Gaps may, however, remain in EU financial sector legislation that should be filled to improve the sector's resilience. Before taking such action, supervisory requirements and practices[40] should be studied carefully. This way, best practices in applying general requirements can be identified.

Access to threat intelligence and information sharing are also fundamental to improving cybersecurity. Closer cooperation and coordination of threat intelligence sharing across the EU financial sector will help to prevent and mitigate cyber threats. Some respondents to the FinTech consultation expressed concern that information sharing on cyber threats could be constrained by legislation. It might for example not be compatible with the General Data Protection Regulation. This Regulation, however, recognises that the processing of personal data necessary and proportionate for the purpose of ensuring network and information security constitutes a legitimate interest.

Supervisors are increasingly conducting penetration and resilience testing to assess the effectiveness of cyber defences and security requirements. Rigorous testing is already an industry best practice, and increasingly tests and testing modalities are mandated by authorities. As financial institutions and financial market infrastructures operate on a cross-border basis, the multiplication of testing frameworks is perceived as increasing the costs unnecessarily and increasing potentially the risks. Stakeholders stressed the need for more regulatory and supervisory coordination at European level. They stated this should be combined with stronger cooperation between jurisdictions and mutual reliance between authorities on test results whose sensitive nature had to be protected. In this context, the Commission considers the efforts that the ECB, the ESAs and national supervisors are making for example to develop an EU-wide *Threat Intelligence Based Ethical Red Teaming (TIBER-EU)* testing framework as promising. Assessing cyber resilience of significant financial

[37] 'Report on FinTech: the influence of technology on the future of the financial sector', Committee on Economic and Monetary Affairs, Rapporteur: Cora van Nieuwenhuizen, 2016/2243(INI), 28 April 2017.

[38] ENISA, *Review of the Cyber Hygiene practices*, December 2016, p.14, available here.

Cyber hygiene is a fundamental principle relating to information security […],is the equivalent of establishing simple routine measures to minimise the risks from cyber threats. The underlying assumption is that good cyber hygiene practices can drive increased immunity across businesses reducing the risk that one vulnerable organisation will be used to either mount attacks or compromise a supply chain.

[39] Directive (EU) 2016/1148.

[40] Financial Stability Board, *Stocktake of publicly released cybersecurity regulations, guidance and supervisory practices*, October 2017, pp. 65-70, available here (tbc).

market players across the EU financial sector has the potential to efficiently and effectively identify vulnerabilities of the stability and integrity of the entire EU financial system.

Strong cyber resilience requires a collective and wide-ranging approach as well as effective training and awareness-raising activities. For this, the Commission has recently adopted its *Digital Education Action Plan* to improve digital skills throughout Europe, including for cybersecurity[41]. The inherent global nature of cyber threats has made clear that international cooperation is crucial to address such risks: for this reason, the Commission is actively involved in the G20 and G7 work on cyber security in financial services.

Box 8

1. **The Commission will organise a public-private workshop in Q2 2018 to explore and assess barriers limiting information sharing on cyber threats between financial market participants and to identify potential solutions while ensuring data protection standards are met.**

2. **The Commission invites the ESAs to map, by Q1 2019, the existing supervisory practices across financial sectors around ICT security and governance requirements, and where appropriate: a) to consider issuing guidelines aimed at supervisory convergence and enforcement of ICT risk management and mitigation requirements in the EU financial sector and, b) if necessary, provide the Commission with technical advice on the need for legislative improvements.**

3. **The Commission invites the ESAs to evaluate, by Q4 2018, the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector.**

CONCLUSIONS

The rapid advance of FinTech is driving structural changes in the financial sector. In such a fast-moving environment, overly prescriptive and precipitous regulation carries the risk of undesired outcomes. However, there are also risks that refraining from updating policy and regulatory frameworks may place EU financial service providers at a disadvantage in an increasingly global market. There is also the possibility, for example in the case of cyber security, that key risks remain unaddressed.

[41] Action 7 in the digital education action plan is aimed at tackling the challenges of digital transformation by launching: (i) an EU-wide awareness campaign targeting educators, parents and learners to foster online safety, cyber hygiene and media literacy; and (ii) a cyber-security teaching initiative building on the digital competence framework for citizens, to empower people to use technology confidently and responsibly.

This FinTech action plan combines both supportive measures to help introduce FinTech solutions and proactive measures to foster and stimulate new solutions and address in a determined way the emerging risks and challenges. The Commission has set out its plans for further work on enabling, accommodating and, where possible, encouraging innovation in the financial sector, while ensuring at all times the preservation of financial stability and high levels of investor and consumer protection. It is one important pillar of a broader strategic approach to regulation in the post-crisis environment. The goals are threefold: to harness rapid advances in technology for the benefit of the EU economy, citizens and industry, to foster a more competitive and innovative European financial sector, and to ensure the integrity of the EU financial system.