European Commission

Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG)

# 30 RECOMMENDATIONS ON REGULATION, INNOVATION AND FINANCE

Final Report to the European Commission

December 2019

Banking and Finance

**An interactive version of this publication, containing links to online content, is available in PDF format at:**

https://europa.eu/!yu87Xf

*scan QR code to download*

**Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG):**

**30 Recommendations on Regulation, Innovation and Finance -**

***Final Report to the European Commission - December 2019***

European Commission

Directorate-General for Financial Stability, Financial Services and Capital Markets Union

European Commission

1049 Bruxelles/Brussel

Belgium



CREDITS

All images © European Union

# Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG)

# Thirty Recommendations on Regulation, Innovation and Finance

Final Report to the European Commission

13 December 2019

Table of Contents

***Avant-propos*** ..... ***5***

***Participants in the work of the ROFI Expert Group*** ..... ***7***

***Executive Summary*** ..... ***9***

Benefits of an accommodative framework for FinTech in the EU ..... 10

Risks and safeguards ..... 10

Competitiveness and sovereignty of the EU as a global standard setter ..... 11

The approach at the basis of this report ..... 12

The core findings of the Group ..... 13

***Complete List of Recommendations*** ..... ***15***

***Introduction: Setting the Scene – The Innovative Use of Digital Technology in Finance*** ..... ***22***

***The FinTech Technological Space*** ..... ***27***

*Artificial Intelligence* ..... *28*

*Blockchain/Distributed Ledger Technologies* ..... *31*

*Blockchain explained* ..... *32*

*How DLT and Blockchain relate to each other* ..... *33*

*Smart Contracts* ..... *33*

*Quantum computing* ..... *35*

*Internet of Things: enhanced consumer data and transactions* ..... *36*

***Recommendations and Background*** ..... ***38***

***Innovative use of technology in finance*** ..... ***38***

*Understanding technology and its impact* ..... *38*

*Cyber Resilience* ..... *43*

*Outsourcing* ..... *44*

*Governance of distributed financial networks; legal framework for crypto-assets* ..... *47*

*Standardisation, RegTech and SupTech* ..... *60*

***Maintaining a Level Playing Field*** ..... ***67***

*Regulatory approach* ..... *67*

*End fragmentation, especially regarding KYC* ..... *72*

*Access to infrastructures* ..... *79*

*Limitation of scope of business* ..... *80*

***Access to data*** ..... ***84***

***Financial inclusion and ethical use of data*** ..... ***90***

***Conclusion – Establishing priorities in regulating FinTech*** ..... ***95***

***Glossary of Acronyms*** ..... ***97***

# Avant-propos

*This report constitutes the outcome of our group's work to identify regulatory obstacles to financial innovation and recommendations to address these issues.*

*We were given the mandate to prepare this report by the European Commission in spring 2018. On the basis of applications received from an open call for applications[1], the Commission decided on the composition of the group and chose members as experts in our respective fields and as representatives of different groups of stakeholders, notably, of incumbent financial institutions such as banks and insurance companies, of new entrants into the financial market and their financiers, members of academia and of the legal profession. The work was enriched by observers representing EBA, EIOPA, ESMA, and the ECB and CPMI whom the European Commission also invited to participate in the group. We were aided by staff of the European Commission services.*

*We held twelve full-day meetings at the premises of the European Commission between June 2018 and October 2019, and a significant number of video conferences in between these meetings and before the finalisation of the report. Our group's dedication to this process was extraordinary, as manifested by the amount of time they invested into our deliberations (the attendance rate for our meetings was above 80% overall) and into drafting, as a collegiate, the relevant sections of our report. For most of us, the time commitment to the group came on top of our regular commitments, and involved, in some cases, significant travel.*

*With this report, we present our "Thirty Recommendations" on how to create an accommodative framework for technology-enabled provision of financial services ('FinTech') in the EU. They cover all segments of the financial sector, all types of novel technologies, a wide range of business cases currently observed and all types of market players. They also span important policy areas, including the prevention of money laundering and terrorist financing ('AML/CFT'), consumer protection, data sharing and use, and governance and operational resilience within the financial sector. Thus, our work has an extremely broad scope.*

*We opted for this all-encompassing approach in order to avoid that sectoral action (i.e. Recommendations for specific market segments, etc.) would risk additional regulatory fragmentation, given the potential applications of technologies within (and outside) the financial sector. Our Recommendations are supported by an analysis of the various uses of technologies when it comes to providing financial services, designing financial products or performing other functions in the financial markets, such as AML checks, and supervising the financial sector.*

*None of our Recommendations are quick fixes. Some may even be rather complex in terms of implementation. Still, we are convinced that the EU should not restrict its actions to the low hanging fruit, but should pursue an approach which seeks to ensure that it remains competitive in this area, offering choices to consumers and businesses while at the same time appropriately mitigating associated risks.*

*Philipp Paech, Chairman*

*13 December 2019*

[1] See: https://ec.europa.eu/info/publications/180308-fintech-call-for-applications_en.

# Participants in the work of the ROFI Expert Group

**Members**

| | |
|---|---|
| Philipp PAECH ***(chairman)*** | London School of Economics and Political Science |
| Hubert BERLIER DE VAUPLANE | Kramer Levin Naftalis & Frankel |
| Tom BUTLER | University College Cork |
| Michael COLETTA | London Stock Exchange Group |
| Thomas JANTSCH | Munich Re |
| Sandra KUMHOFER | FinLeap GmbH |
| Christian LANGE-HAUSSTEIN | German Savings Banks Association |
| Benoît LEGRAND | ING |
| Simon MAISEY | Tradeweb Europe |
| Alvaro MARTÍN ENRÍQUEZ | BBVA |
| Alexandra SALANSON | Axa Group |
| Nicole SANDLER | Barclays |
| Antonella SCIARRONE ALIBRANDI | Universita Cattolica del Sacro Cuore |
| Sofie VAN DE VELDE | Euroclear |
| Bruno VAN HAETSDAELE | Linxo Group |

**Observers**

| | |
|---|---|
| Elisabeth NOBLE | European Banking Authority |
| Julian AREVALO CARRENO | European Insurance & Occupational Pensions Authority |
| Patrick ARMSTRONG | European Securities & Markets Authority |
| Johanne EVRARD | European Central Bank |
| Klaus LÖBER | Committee on Payments and Market Infrastructures |

**Secretariat**

| | |
|---|---|
| Tobias MACKIE | European Commission DG FISMA |
| Dora KOVACS | European Commission DG FISMA |

**Research assistant**

| | |
|---|---|
| Rocco STEFFENONI | Bocconi University |

# Executive Summary

In the EU, technology-enabled innovation in the financial sector ('FinTech') is driving the emergence of new business models, applications, processes and products. Indeed, FinTech could have real impact on financial markets and institutions and how financial services are provided.[2] Technology-enabled financial services are provided by different types of market participant: incumbents (banks, insurers, investment firms, pension funds, financial infrastructures, etc.); big non-financial firms, (including the so called BigTechs, such as internet search and advertising companies, device manufacturers, commercial platforms, but also telecoms operators) and by start-ups. They design technology-enabled financial services for use on the Internet and on mobile devices, combined with other recent technologies, such as cloud computing, distributed ledger or blockchain technology, or Artificial Intelligence (AI). The results have a lesser or greater degree of originality, some heavily resemble well-known services and products (such as mobile payments), others appear to break new ground (such as crypto-assets, initial coin offerings, or automated investment advice).

Our Expert Group has been established by the European Commission, in accordance with its 2018 FinTech Action Plan, to review the application and suitability of the European legal and regulatory framework to FinTech in order to identify issues that may impede the scaling-up of FinTech in the EU. We were asked to analyse the extent to which the current framework for financial services is technology-neutral and able to accommodate FinTech innovation and whether it needs to be adapted, also with a view to making the framework future-proof. At the same time, we were asked to consider how financial stability, financial integrity, and consumer and investor protection can be ensured in light of the new opportunities and risks afforded by FinTech.[3]

Our Group is aware that many technological innovations, such as AI, Big Data and DLT/Blockchain, have uses beyond finance, in very different areas of economic and social life and across the public sector. For this reason, it is relevant to consider changes to the general regulatory framework (across multiple industry sectors), as well as the framework for the regulation of the financial services sector, which may require tailored responses in order to be able to realise the potential of specific opportunities and to take account of specific regulatory concerns in an already highly regulated environment.

In particular, there are universal aspects, such as ethical considerations, where finance sector-specific approaches and those in other areas of life merit special attention in order to ensure consistency. One example may be the use of AI and Big Data in the context of client interfaces (robo advice, chatbots, insurance pricing and underwriting, credit scoring, or certain other

[2] See: http://www.fsb.org/what-we-do/policy-development/additional-policy-areas/monitoring-of-FinTech and https://www.fsb.org/2019/12/fsb-reports-consider-financial-stability-implications-of-bigtech-in-finance-and-third-party-dependencies-in-cloud-services/ .

[3] European Commission 2018 FinTech Action Plan, p. 10.

applications) – where we are facing similar ethics-related issues as in other areas of life, such as healthcare.

## Benefits of an accommodative framework for FinTech in the EU

The potential gain to be derived from furthering the use of FinTech in the EU is often described as 'higher efficiency'. Our Group divides those gains into four different aspects:

- FinTech may enable market participants to provide financial services at lower cost (disruption of traditional value chains; disintermediation; further automatisation resulting in more efficient processes);
- FinTech may enable market participants to develop a broader range of products and services, thereby widening consumers' and businesses' choice and potentially providing them with better financing opportunities (new and better products and services such as crypto-assets, P2P/B2B lending);
- FinTech may open certain products or services to consumers or businesses that were previously excluded, due to a higher degree of personalisation, broader product offerings, better pricing through lower marginal cost and improved accuracy of credit scoring;
- FinTech may be used to achieve more effective regulation and compliance of the relevant market players (automated reporting, data analysis, transactions monitoring).

As things currently stand, such benefits cannot be realised fully by European market participants. This is, to a significant extent, due to an absent, fragmented or unclear regulatory framework. Our Group agrees that harmonising and clarifying regulatory and supervisory measures will provide an effective tool to support the scaling up of FinTech across the EU. As a consequence, we have interpreted our mandate in relation to this unused potential so as to:

**Identify obstacles to the adoption of FinTech in the EU (Task 1);**

**Identify obstacles to the scaling-up of FinTech across the Single Market, including with a view to enhancing the global competitiveness of the EU (Task 2).**

## Risks and safeguards

Many of the potential risks emerging as a consequence of the use of FinTech are no different from the risks caused by the provision of financial services using more traditional means (indeed, our Group is mindful of the fact that it is not possible to draw a clear line between 'traditional' and 'innovative' finance).

The fact that financial services are increasingly enabled by technology may increase or diminish these traditional risks:

- Consumers and businesses are subject to intermediary, settlement or custody risk, exposing them to the possibility of losing assets in case of, for example, operational failure, insolvency or malpractice on the side of the custodians that keep their assets;
- Consumers and businesses are exposed to principal-agent risk, i.e. the risk that their agent provides suboptimal advice or services (investment decisions, order execution);
- The market as a whole is vulnerable to systemic risk, i.e. a chain reaction of adverse market developments, such as liquidity shortages or flash crashes, that might threaten the proper functioning of the market;
- The financial market, like other areas, creates the potential for activities that contravene market integrity (e.g. market manipulation), or for criminal abuse (money laundering, tax evasion, purchase of illegal goods or services, etc.).

However, the use of FinTech may also create entirely new risks, for instance, where:

- Decisions are taken, or functions are performed by AI-powered 'black box' algorithms without human intervention or which are not comprehensible to customers or supervisors;
- Distributed record keeping or transaction processing blurs regulatory and legal responsibilities that were traditionally based on bilateral principal-agent relationships.

Against this background, our Group has interpreted its mandate so as to include two tasks in respect of detecting risks and proposing safeguards:

> **Clarify whether existing safeguards addressing specific risks can be applied smoothly to the new technology-based environment where it poses similar risks, or whether clarification or adaptation might be necessary (Task 3);**
>
> **Identify whether the emergence of FinTech poses any entirely new risks that would necessitate new safeguards (Task 4).**

## Competitiveness and sovereignty of the EU as a global standard setter

Efficiency and safety must be considered in light of the need to ensure the global competitiveness of the EU financial sector. The EU needs to keep pace with the application of new technological developments and the setting of relevant regulatory standards in the financial sector in order to remain competitive in a global financial market. The current distribution by home region of the value of technology companies reveals the big gap that exists between the EU on the one hand (5%) and the US (65%) and the PR China (35%) on the other.[4]

More ambitiously, the EU should take a proactive lead in responding to these developments, so that it can help shape the global technology-enabled financial market, thereby promoting its fundamental European values, such as data privacy and fair competition. Both data protection

[4] Howard Covington, *Glimpsing our AI Future*, Lecture, The Alan Turing Institute, 28 January 2019. The data relates to technology companies with a market capitalisation >10bn USD.

and competition law may be perceived by some as inhibitors of a rapid uptake of FinTech, notably because fast developing non-EU financial markets operate under considerably less stringent standards than European markets. However, if calibrated appropriately, the Group regards these areas of law, in the long run, to offer the means of protecting its values whilst not posing an undue barrier to the innovative use of technologies.

At the same time, to safeguard its own sovereignty it is vital that the EU maintains its role as one of the key global standard-setters also in relation to FinTech, and the Group views opportunities for the EU to provide genuine thought leadership for the regulation of innovative technology within and beyond the financial sector. In so doing, it is important for the EU to follow developments in other jurisdictions and engage with other regulators, supervisors and international standard-setting bodies in order to facilitate interoperability of technology across jurisdictions, in line with common standards.

Global champions typically start growing on their home turf. They need to establish a sufficiently large pool of potential customers before they can scale up their business. Only then can they build up the financial resources, resilience and innovation power to be able to expand internationally and globally. However, fragmentation of the local customer base in terms of law and regulation will hold them back: aspiring global service providers in the EU have to deal with different legal and regulatory frameworks already across the internal market, i.e. the (fragmented) laws of all Member States. **In short, competitiveness and regulatory sovereignty in relation to technology-driven finance require a considerably more harmonised framework on the basis of existing regulatory axioms than currently exists in the EU.**

Adapting existing rules to a changing market and ending the fragmentation of the EU regulatory environment are certainly not the only determining factors for the healthy and dynamic development of FinTech. Other factors, which are beyond the remit of this report, include the availability of a specialised workforce, a tradition of availability of venture capital, taxation, and the fact that relevant technologies and infrastructures have for some time been concentrated in other parts of the world.

## The approach at the basis of this report

Setting the right level of financial regulation and financial supervision requires addressing highly antagonistic rationales: increasing efficiency through technological innovation may put safety and protections under strain, and, conversely, a higher degree of safety often comes at a higher compliance cost. We hence strive to make proposals for changes to the European regulatory and supervisory framework that balances both aims (and noting the interactions with relevant central bank oversight frameworks).

We endorse the concept of technological neutrality of financial regulation and supervision, which we interpret to mean that typically regulation and supervision should not prefer or prejudice a specific provider or technology. Hence, we try to avoid making any recommendations aiming at technology-specific rules or recommending any steps to be taken

to specifically address issues in relation to specific technologies. In our view, technology-specific regulation would render the regulatory architecture complex and inconsistent. That said, the Group recognises that sometimes, regulatory and supervisory approaches should be informed by the opportunities and risks presented by new technological paradigms which can still be specifically considered, regulated and supervised. Therefore, the Group has put forward some Recommendations that relate to specific technologies, notably AI and DLT/Blockchain.

As such, our output consists of:

**Thirty Recommendations which embody common regulatory and supervisory themes. They are not specific to any business model or financial service or product and cut across the whole market. We regard them as the fundamental issues to be addressed with a view to dismantling obstacles and opening opportunities for FinTech in the EU.**

## The core findings of the Group

Our Thirty Recommendations are set out in the following pages (and repeated together with their background later on in this report). They can be grouped into four categories

- First, the need to adapt regulation to respond to new and changed risks caused by the use of innovative technologies, such as AI and DLT, and take up any emerging opportunities with respect to RegTech or SupTech (Recommendations 1-12);
- Second, the need to remove regulatory fragmentation and ensure a level playing field between incumbents and new market entrants, both FinTech start-ups and BigTech firms, across the entire EU (Recommendations 13-24);
- Third, the necessity to reconcile the regulation of personal and non-personal data with the opportunities and risks offered by FinTech (Recommendation 25-28);
- Fourth, the need to consider the potential impacts of FinTech from the perspective of financial inclusion and the ethical use of data (Recommendations 1 and 29-30).

In the concluding chapter of this report, we indicate our top Recommendations in terms of regulatory reform, highlighting the need to address as a matter of priority:

- The explainability and interpretability of technology, especially AI, as measures to protect consumers and businesses and facilitate supervision, or to meet supervisory expectations (Recommendation 1);
- The creation of a regulatory framework built on the principle that activities that create the same risks should be governed by the same rules, with a view to ensuring adequate regulation and supervision and maintaining a level playing field (Recommendation 13);
- The ending of regulatory fragmentation, especially in the area of customer due diligence (CDD)/know your customer (KYC), as an important step towards creating a level playing field (Recommendations 15-17);

- Preventing unfair treatment of competing downstream services by large, vertically integrated platforms, in order to strengthen innovation and maintain consumer choices (Recommendation 22);
- The strengthening of the framework for access to, processing and sharing of data, in order to promote innovation and competition and establish a level playing field amongst actors (Recommendations 27 and 28).

The Group stresses that the aims informing these and all other Recommendations are best pursued by regulation that is neutral, in the sense that it does not differentiate between the different technologies that can potentially be used to provide a service, offer a product or perform a function. The Group further believes that international cooperation in setting relevant standards, ideally leading to interoperability, is crucial.

# Complete List of Recommendations

## Innovative use of technology in finance

*Recommendation 1 – Explainability and interpretability of AI and associated technologies*

*The Commission should, in co-operation with the ESAs and relevant international standard-setting bodies:*

- *develop measures clarifying the circumstances under which requirements aiming at explainability or interpretability of AI and associated technologies, in their concrete applications, are appropriate, considering the need for sector-specific or horizontal rules;*
- *provide guidance on how to meet explainability and interpretability requirements, where applicable, in respect of different stakeholders, including consumers and supervisors, acknowledging that different standards will be needed depending on the type of application for which the relevant technology is being used.*

*Recommendation 2 – Firms' internal IT governance*

*The Commission should, in cooperation with the ESAs, require regulated entities to build adequate levels of IT governance and technological expertise at the appropriate management level, including, where appropriate, at board level.*

*Recommendation 3 – Supervisors' understanding of technology*

*The ESAs should be given a mandate to encourage and support supervisors in developing appropriate internal understanding, at appropriate levels, of the use of technology in financial services and the potential associated risks and opportunities.*

*Recommendation 4 – Cyber resilience*

*The Commission should, in cooperation with the ESAs and the ESCB, develop a coherent and proportionate cyber resilience testing framework for the financial sector.*

*Recommendation 5 – Outsourcing guidelines and certification/licensing*

*The Commission, in cooperation with the ESAs and the ESCB, international standard-setting bodies and other relevant authorities, should regularly monitor the extent and structure of outsourcing of critical services by financial institutions, and assess the appropriateness of tools in place to mitigate concentration risks, operational risks and systemic risk, taking account of the potential impact on innovation and competition. On this basis:*

- *the ESAs should regularly review the outsourcing guidelines with a view to maintaining their proportionality in light of technological developments, new risks and new market conditions;*
- *the Commission, in cooperation with the ESAs, should consider the need to introduce a certification or licensing regime for third parties providing technology services to regulated entities.*

*Recommendation 6 – Distributed financial networks*

*The Commission, in co-operation with the ESAs, the ESCB and international standard-setting bodies and other relevant authorities, should take action to clarify the regulatory framework applicable to distributed financial networks, in particular to:*

a. *assess and clarify how relationships between participants should be regarded for regulatory and supervisory purposes, taking account of existing concepts such as agency and outsourcing;*
b. *ensure the applicability of defined terms and established concepts in existing regulation, such as SFD, FCD, CSDR, EMIR, MiFID, the SIPS Regulation or AMLD in view of the shift from bilateral relationships to a multilateral environment where functions can be attributed simultaneously to several parties;*
c. *define the addressee of relevant regulation concerning distributed financial networks;*
d. *assess and clarify how issues of operational resilience and higher exposure to cyber risks (in particular with regard to private key management) or systemic network failures, should be addressed.*

*Recommendation 7 – Crypto-assets*

*The Commission, in co-operation with the ESAs, the ESCB and international standard-setting bodies and other relevant authorities should accelerate its work to assess the adequacy and suitability of existing rules mitigating risk flowing from the use of crypto-assets in the context of the provision of financial services and on this basis develop a legislative solution to complement and complete the framework where necessary. This process should extend to addressing:*

a. *the risk and uncertainty flowing from the lack of a common taxonomy in respect of crypto-assets and the consequential fragmented national approaches to classifying crypto-assets under EU rules, such as MiFID or the e-money Directive and emerging national law;*
b. *the risks flowing from activities involving crypto-assets, in particular, in relation to:*
    - *money laundering, terrorist financing and tax evasion;*
    - *governance and operational resilience;*

- *client asset protection, including regarding segregation of client assets, redemption rules, disclosure requirements, and consumers' interests;*
- *systemic effects, including through threats to the orderly functioning of the payment environment;*
- *the prudential treatment of regulated financial institutions' exposures to crypto-assets;*
- *pegging and foreign exchange conversion mechanisms.*

*Recommendation 8 – Commercial law of crypto-assets*

*In order to ensure market participants' rights and to guarantee a meaningful application of the commercial law concepts established in EU regulation (such as InsR, SFD, FCD, BWUD, BRRD) to crypto-assets which are held on a distributed financial network, the Commission, in co-operation with the ESAs and international standard-setting bodies and other relevant authorities, should:*

a. *legislate a relevant conflict-of-laws rule, ideally enshrined in a Regulation, and,*
b. *consider which further aspects of the commercial law regarding such networks and regarding the assets administered on them should be addressed at EU level.*

*Recommendation 9 – RegTech and SupTech*

*The Commission, in cooperation with the ESAs, and in co-ordination with relevant authorities and international standard setters, should develop and implement a comprehensive and ambitious agenda to support the adoption of advanced RegTech and SupTech by the financial sector.*

*Recommendation 10 – Standardisation of legal terminology and classification of actors, services, products and processes*

*The Commission, in co-operation with the ESAs and the ESCB, should facilitate initiatives that promote standardisation of legal terminology and digital standards-based common classifications of actors, services, products and processes in the financial sector for use by market participants, regulators, supervisors and standard setters.*

*Recommendation 11 – Human- and machine-readable legal and regulatory language*

*The Commission, in co-operation with the ESAs, should adopt a strategy on how reporting and compliance processes may become both machine- and human-readable, to the extent possible.*

*Recommendation 12 – Regulatory Clearing House*

*The Commission, in co-operation with the ESAs and the ESCB, should adopt a strategy for the conception and establishment of regulatory clearing houses, i.e. arrangements capable of:*

- *centralising the automated dissemination of rules to regulated entities,*
- *receiving incident and reporting information from regulated entities, and*
- *collecting market data.*

## Maintaining a Level Playing Field

*Recommendation 13: Activity and risk-based regulation*

*The Commission and the ESAs should take the necessary steps to ensure that regulation of the financial sector follows the principle of 'same activity creating the same risks should be regulated by the same rules'.*

*Recommendation 14 – EU-level facilitation, including 'the sandbox'*

*The Commission and the ESAs should further assess the need to establish an EU-level 'regulatory sandbox', or similar scheme, taking account of the experience acquired in the context of European Forum for Innovation Facilitators.*

*Recommendation 15 – Uniform regulation*

*The Commission, in co-operation with the ESAs, should review the aspects of financial regulation that are currently subject to fragmented regulation and assess how to address them to ensure the highest possible uniformity across the EU in order to foster efficiency and competitiveness.*

*Recommendation 16 – Fully harmonised KYC processes and requirements*

*The Commission, in co-operation with the EBA, should introduce legislation to fully harmonise the Know Your Customer (KYC) processes and requirements across the EU for obliged entities in the financial sector according to the AMLD with regard to identification and verification processes, as well as the mandatory collected set of data.*

*Recommendation 17 – Convergence in the use of innovative technologies for CDD purposes*

*The Commission and the EBA should take steps to achieve convergence in the acceptance, regulation and supervision of the use of innovative technologies for CDD purposes, including remote customer onboarding, and consider them on their respective merits, including through:*

- *enhanced industry engagement and monitoring of market developments;*

- *periodic updates of the Risk Factor Guidelines to support the use of these innovative technologies;*
- *further guidance relating to reliance on third parties, including on issues relating to liability;*
- *changes to Level 1 legislation (e.g. the AMLD), based on the advice of the EBA).*

*Recommendation 18 – Clarifying the capacity to re-use CDD data*

*The Commission, in cooperation with the EDPB and the EBA, should clarify the rights of data subjects to permit the use of data provided for CDD purposes and the outcome of identity verification for further identified purposes, where the data subject consents.*

*Recommendation 19 – Digital identity verification*

*The Commission, in consultation with the EBA and relevant authorities, should investigate potential models (including decentralised models) for efficient, robust and trusted digital identity verification. The findings should inform a future legislative strategy on common digital identity solutions in the EU.*

*Recommendation 20 – End default paper requirement*

*The Commission, in cooperation with the ESAs, should take steps to remove provisions of financial services law that require documentation to be provided, by default, to consumers in hard copy. This is without prejudice to the right of consumers to request information in this format.*

*Recommendation 21 – Participation in clearing and settlement systems*

*The Commission, in cooperation with the ESAs and the ESCB, should evaluate the need to revise the Settlement Finality Directive to allow for the participation in clearing and settlement and payment systems of any type of regulated financial institution, on the basis of appropriate risk-based criteria.*

*Recommendation 22 – Access to platforms*

*The Commission should introduce rules to ensure that large, vertically integrated platforms do not unfairly discriminate against downstream services that compete against their own similar services.*

*Recommendation 23 – Framework for P2P insurance*

*The Commission, in cooperation with EIOPA, should evaluate the need for a framework for the regulation of P2P insurance.*

*Recommendation 24 – Proportionate restrictions on non-core business*

*The Commission, in cooperation with the ESAs and the ESCB, should consider the impact of existing activities restrictions for financial institutions' non-core business, to determine whether these restrictions remain proportionate and, if so, whether the restrictions are consistently applied having regard to the need to maintain a level playing field.*

## Access to data

*Recommendation 25 – GDPR and new applications of technology*

*The EDPB should issue guidance on the application of the GDPR and other relevant legislation, in relation to the innovative use of technology in financial services, including the use of:*

- *DLT/Blockchain, in particular how to satisfy the requirement for erasure, for example, using encryption;*
- *Artificial Intelligence, in particular addressing the issue of specificity of consent.*

*Recommendation 26 – Regulatory Dialogue*

*The regular dialogue between the European Data Protection Board, the European Forum for Innovation Facilitators, national data protection authorities, national and EU competition authorities, national and EU financial regulators and financial supervisors and firms should be extended, with a view to keeping under review the practical application of relevant EU legislation concerning the processing of data (in particular GDPR and PSD2), taking account of technological developments within and beyond the financial sector. The objectives of this dialogue should be to:*

- *enhance knowledge-sharing about new technologies;*
- *share experiences and promote a common approach to the regulatory and supervisory approach to the practical application of relevant EU legislation concerning the processing of data;*
- *provide where appropriate clarification of or guidance on relevant EU legislation concerning the processing of data in a form that is publicly accessible.*

*Recommendation 27 – Access to and processing of non-personal data*

*The Commission should develop measures to provide legal certainty on the access to and processing of non-personal data by different stakeholders. In preparing these measures, the Commission should assess the need for an EU-level supervision and enforcement mechanism and ensure consistency across the EU.*

*Recommendation 28 – Data sharing*

*The Commission should introduce rules to ensure that a user of digitally enabled products or services has the possibility to share seamlessly, securely and in real-time with other market participants of their choice the data that the providers of those products or services have observed on them. These rules should support user control and data-driven innovation by ensuring sharing is easy, secure and effective, for example by mandating the use of standardised sharing interfaces.*

## Financial inclusion and ethical use of data

*Recommendation 29 – Financial inclusion and exclusion*

*The European Commission, in cooperation with the ESAs, should monitor and have regard to the impact of the increasing use of technology-driven financial services on our society and, where significant issues arise, should take action to:*

- *promote the use of those technology-driven financial services as a means to address financial inclusion;*
- *prevent the use of those technology-driven financial services in ways that exacerbate financial exclusion or causes unfair discrimination.*

*Recommendation 30 – Ethical use of data*

*The Commission, should, in cooperation with the ESAs and the EDPB, develop guidance to assist financial institutions in the ethical use of data in the context of the provision of financial services.*

# Introduction: Setting the Scene – The Innovative Use of Digital Technology in Finance

Financial Technology (FinTech) enables:

a. the provision of financial products and services;

b. the development of new innovative financial products and services; and

c. the digitalisation and re-engineering of front-, middle- and back-office processes, in and across financial institutions, to make them more efficient and effective.[5]

FinTech is by no means a new phenomenon, as technology has supported financial processes since the telegraph was first used to wire transfers of money in the 19th century. Since the 1950s, however, computer and telecommunications technologies have transformed the financial services sector and how consumers and businesses interact with it. From ATMs to card readers, e-banking and e-trading to high frequency trading, technologies have shaped and disrupted the financial industry for quite some time.[6]

Financial institutions, whether incumbents or start-ups, are providing new products and services using established digital technologies, such as smartphones and cloud computing, and a range of Internet-based applications. Beyond these fairly ubiquitous uses of technology in finance, consumers and businesses have encountered digital innovations, such as chatbots that advise on financial matters, automated paper-less opening of bank accounts and conclusion of insurance contracts, or payments using crypto-assets.

There are a range of core and enabling digital technologies supporting new business models, products and services. These range from AI technologies, such as machine learning, natural language processing and knowledge representation, to blockchain and distributed ledger technologies (DLT), to new application programming interfaces (APIs), smart contracts and, potentially, quantum computing. None of these were developed with financial innovation in mind; however, their potential use in and consequential impact on the financial sector may be very significant. The *core technologies* underpinning FinTech are discussed below in the section entitled 'The FinTech Technological Space'.

The digital transformation of financial services is driving the FinTech market. Identifying the total expenditure on digital technology across the industry, and therefore the market size, is difficult. In 2019, Accenture reported that the 161 largest retail and commercial banks spent over $1 trillion over three years to 2019 on digital technology.[7] However, the authors point out that just 19 banks are committed to leveraging the benefits of digital transformation at scale. Thus, the global expenditure on digital technology by the largest banks globally is

---

[5] See a similar definition adopted by the FSB, http://www.fsb.org/what-we-do/policy-development/additional-policy-areas/monitoring-of-FinTech/

[6] Arner, D. W., Barberis, J., & Buckley, R. P.. *The evolution of FinTech: A new post-crisis paradigm*. Geo. J. Int'l L., 47, 1271 (2015).

[7] Accenture (2019). https://www.accenture.com/_acnmedia/pdf-102/accenture-banking-does-digital-leadership-matter.pdf

approximately $350 billion. Given that the number of licensed banks globally is estimated at approximately 25,000, with another circa 60,000 'quasi' banks,[8] the total spend on digital technology may be breath-takingly large. In contrast, the global annual expenditure on digital technology by the insurance sector is estimated at $185 billion.[9] Of this, over €70 billion or 39% was spent by European insurance companies on digital technologies. We estimate that the total spend by the largest financial institutions globally is approximately $535 billion, with approximately €192 billion of this spent in Europe. However, the true size of the European market for digital technology is much greater, given the number of smaller banks and 'quasi' banks. Thus, the opportunities for growing the European FinTech sector are significant, as more and more financial institutions undergo true digital transformation in order to remain competitive.[10] While existing digital technology vendors provide enabling and supplemental technologies, digital innovation will increasingly be sourced from FinTech enterprises.

The European FinTech market is dynamic and its footprint can be observed to a greater or lesser degree in all EU Member States. Overall, during the first half of 2019, investment in European FinTech start-ups alone (including mergers and acquisitions) amounted to $13.2 billion: while continuing its upward growth trend, the market is consolidating and venture capital investment in FinTech remains strong.[11] The KPMG report (ibid.) indicates that future investment will focus in particular on digitisation of securities and other financial assets, and increasing interest in digital comparison platforms for banking and other forms of financial services can also be expected. The report indicates that digital banking is gathering momentum, as challenger banks focus on expanding their markets with new business models. Meanwhile, established European financial institutions continue their transformation to digital enterprises internally or in partnership with technology companies.[12]

The use of the digital technologies is disrupting existing value chains across the financial services sector, chiefly because it is exposing the industry to increased competition, through innovative digital business models, and by empowering consumers and businesses in novel and engaging ways, increasing access, trust and overall efficiencies.

Innovation produces new ways of offering financial services in all areas traditionally pertaining to financial sectors, including new ways of organising infrastructures (such as stock exchanges), digital financial assets and digital 'money', different ways to initiate and process payments, tailor-made insurance products, robots providing financial advice and managing portfolios, algorithms calculating credit scorings on the basis of social network data, platforms enabling peer-to-peer lending, and, also, one-stop-online shopping for all types of financial and non-financial products and services.

At the same time, innovation is revolutionising those parts of finance that do not face customers, back office functions such as customer due diligence and compliance and reporting solutions

---

[88] https://www.linkedin.com/pulse/how-many-banks-globally-david-gyori/

[9] Celent (2017). https://www.celent.com/insights/980614747

[10] http://collections.exus.co.uk/blog/digital-transformation-european-banks

[11] KPMG (2019).https://home.kpmg/xx/en/home/campaigns/2019/07/pulse-of-fintech-h1-19-europe.html

[12] https://www.gfmag.com/magazine/may-2019/best-banks-western-europe-2019-digital-transformation-drives-growth

for prudential and other regulation. Additionally, FinTech has the potential to contribute to sustainable finance (for instance, the use of Blockchain in the context of green bond issuance, and as a means to create significant operational efficiencies (e.g. in the context of regulatory reporting).

From the perspective of regulatory and supervisory authorities, technology may offer the potential to automate significant parts of the regulatory and supervisory activity and hence keep up with a high-paced and technology-driven market.

It is clear that the financial industry and its service sectors are currently subject to significant regulation. Broadly speaking, existing EU financial regulation is largely technology-neutral, although there are exceptions. Consequently, regulating how FinTech is being employed often involves minor adjustments to the existing regulatory framework in order to ensure that it continues to be both suitable and relevant to innovations and changes in market practices. However, new regulatory measures will need to be introduced where radical departures from current business models and relationships with consumers are enabled by digital technologies employed in FinTech solutions. The guiding principle of regulation should remain unchanged – that is, to find the correct balance between innovations that enable market efficiency, on the one hand, and the prevention or mitigation of risks, both individual and systemic, on the other.

This report considers potential improvements to the regulatory framework for the EU financial sector from four different perspectives:

- First, significant changes to existing regulation or new regulations may be required where the use of novel digital technologies presents additional risks in: (i) the way financial services or products are delivered; or (ii) the manner in which functions, for example risk management, are performed within market participants. For instance, existing regulation governing outsourcing to third parties has been designed on the basis of the understanding that power and control lie with the outsourcer – for example, an insurer buying in cloud services; however, as a consequence of market concentration and other phenomena, an increasing shift of control and power to the outsourcee can be observed. This scenario potentially creates new risks (stemming from market concentration) which are not addressed (and not intended to be addressed) by outsourcing measures. A second point is that the use of novel digital technology leads to market practices for which current regulatory terminology and concepts are not entirely fit for purpose (e.g., in relation to crypto-assets). As a further example, there may now be black box algorithms intervening in automated decision making, making it nearly impossible for concerned customers to review and challenge these automated decisions. It may also be that the lack of transparency creates specific challenges for supervisors in respect of why and how digital models and algorithms perform in a 'black box' solution, including poor governance and poor articulation to supervisors. There are also cases where digital technologies offer significant potential opportunities for firms and supervisors to reduce compliance costs, for example in the case of transaction monitoring tools and automated regulatory reporting and analysis tools. As a matter of imperative, it is also essential that regulators and supervisors have a common and sound understanding of digital technologies and their potential application in the financial

industry in order to regulate and supervise effectively. The need for timely and relevant adaptation of the regulatory framework or appropriate monitoring by the Commission and others is discussed in Section 'Innovative Use of Finance'.

- Second, there may be a need to adapt regulation in order to ensure a level playing field between incumbents and new market entrants and between different types of market participant. It is clear that there is a symbiotic relationship between retail and wholesale banking, and insurance, on one hand, and innovation in digital technologies across the information technology sector, on the other. Both are evolving in mutually beneficial ways, so much so that the more financial institutions digitize their front, middle and back offices, the more they become like technology or software companies. Some of the world's largest banks have, as one of their number indicated, "*more software developers than Google, and more technologists than Microsoft*."[13] Equally, technology companies – big and small – are now offering financial products and services. Indeed, digital technologies are not only driving change in business models of financial institutions and the structure of the industry, they have been doing likewise in firms across private and public sectors. As a consequence, a raft of new entrants now populates the financial industry. In some cases, new entrants are subsidiaries of well-established incumbent financial institutions, whereas in other cases new entrants are start-ups entirely independent from existing financial institutions driving the trend towards disintermediation of financial services. It is evident that FinTech also enables the provision of some products and services that have features that resemble regulated products and services but fall outside the scope of current EU law because it was not designed with these specific products and services in mind. This is the case for certain types of digital asset or the provision of online brokerage in peer-to-peer lending. At the same time, dominant technology companies, particular BigTechs such as Google, Amazon, Facebook and Apple are lining up to enter the financial industry directly, either on the basis of traditional ideas in a new packaging (such as payment apps for smartphones), or bold steps to attract vital market functions, such as payment and customer identification, to their platforms. While innovation-based competition in the financial industry is positive, regardless of who the relevant provider is, EU regulation must ensure a level playing field for incumbent market participants and new entrants in the form of start-ups and BigTechs, by conforming to the 'similar activity, similar risk, same rule' principle - see 'Maintaining a Level Playing Field'.
- Third, the financial industry is data-intensive, spending more per terabyte than any other. The rise of the Internet, e-commerce, and social networking applications has seen an exponential increase in consumer and business data. New AI-based digital technologies, and the emergence of data science to deal with the challenge of Big Data, presents novel ways to perform data analytics and identify with greater granularity and accuracy consumer profiles and preferences. The need to reconcile the possibility to

[13] Anish Bhimani, Chief Information Risk Officer at JPMorgan Chase; https://wallstreetonparade.com/2014/04/jamie-dimon-jpmorgan-employs-30000-programmers/

have access to data and the rules on data protection suggests careful reform, see Section ‘Access to Data’.

- Fourth, technology-driven financial services may have a societal impact, as have other significant market developments. It will inevitably create winners and losers, amongst business and also amongst consumers. Some may benefit from new opportunities offered by greater access to, and new, financial services and products. Others may lose out, as a consequence of not being technically literate or not having access to the necessary devices such as smartphones and computers. This report hence suggests making the use of the potential for furthering financial inclusion, while closely monitoring potential financial exclusion or unfair discrimination. Beyond, there should be guidance regarding the ethical use of data, in particular as regards its provenance, the application for which data is used, and the increasing need to make data of all kinds available to obtain financial services, see section on ‘Financial inclusion and ethical use of data’.

The Group has termed the analysis of potential improvements of regulation in light of these three aspects ‘horizontal’, as it cuts across all types of market participants (incumbent, start-up, financial institution, BigTech etc.), all types of industries (banking, insurance, markets and others), and all types of digital technologies, new and traditional. The resulting Recommendations are, therefore, equally of a horizontal nature.

# The FinTech Technological Space

Financial technology (FinTech) incorporates several recent advances in digital technologies. These include:

1. AI: comprising Machine Learning, Deep Learning and Artificial Neural Networks, Natural Language Processing, and Knowledge Representation;
2. Blockchain/Distributed Ledger Technologies;
3. Smart contracts;
4. Internet of Things;
5. Quantum Computing.

The application of these core digital technologies to develop new business models, products and services, while transforming the way they are delivered, has enormous potential to disrupt the financial industry. Start-ups, BigTech firms, and incumbent financial institutions, are investing heavily in these technologies to create new revenue models, enhance customer relationships and value, or reduce cost through higher degrees of efficiency, particularly through digitisation and automation of analogue processes.

However, while core technologies are capable of causing paradigm shifts in how banks, insurance companies and related financial institutions operate, FinTech is built first and foremost on other, more common, technologies, which we term 'enabling and supplemental technologies.' Core technological capabilities provide a competitive advantage for a disrupting FinTech (e.g. of an EU-based FinTech vs. a US-based FinTech), enabling technologies are necessary but not sufficient for disruption, while supplemental technologies are perfectly imitable and are, essentially, commodities or well-accepted standards.[14]

1. Cyber Security Technologies (Biometrics, cryptographic algorithms, etc.);
2. Data Analytics Applications (Enabling technology based on machine learning and data science);
3. Cloud and Software-as-a-Service (Enabling platform technology paradigm)
4. NoSQL (Enabling technology paradigm involving Graph Databases, and other innovative ways of storing and accessing data);
5. W3C Internet Standards, HTML, XML (XBRL), RDF, OWL, SWRL SQL Technologies (Supplemental Technology Standard);
6. Data lakes (Supplemental Technology);
7. Hadoop (Supplemental Technology);
8. API Application Programming Interfaces (Supplemental Technology).

[14] Leonard, D. (1995). *Wellsprings of knowledge* (p. 65). Boston: Harvard Business School Press.

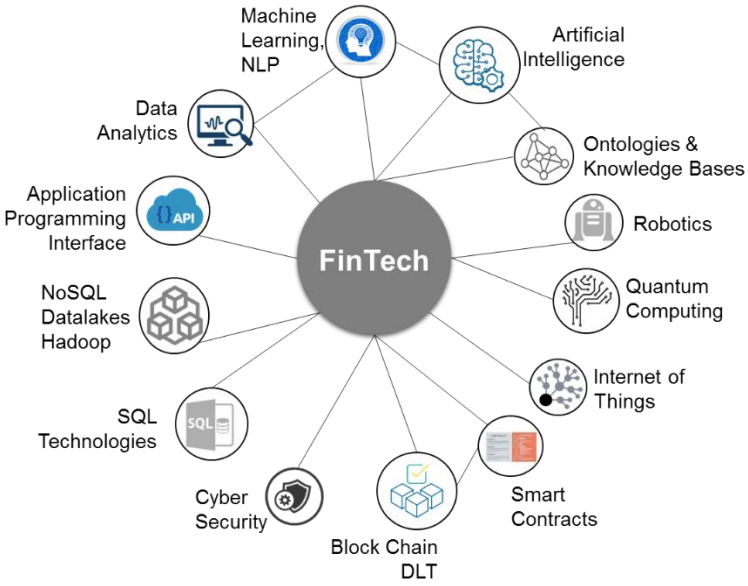


Figure 1: Fintech Technological Space[15]

Enabling technologies are not described in further detail. The core technologies are described in turn below.

## *Artificial Intelligence*

AI will become increasingly relevant for both FinTech and RegTech as it can address both the 'big regulation' and 'big data' problems.

As with other core technologies, recent advances in AI are made possible through more powerful processors, bigger and faster memory and cloud computing.

There are three related AI technology paradigms:

1. Knowledge representation (capturing semantics in models such as 'ontologies'),
2. Natural language processing (NLP),
3. Machine learning (ML) and deep learning (DL) which is a form of ML using artificial neural networks (ANN). The growth and power of machine learning algorithms, natural language processing, and artificial neural networks made weak AI or perceptual computing possible.

Together these paradigms offer great promise in making AI a reality, but they are being used piecemeal. Hence, what is currently possible is called *perceptual computing*: this involves sophisticated digital pattern matching and predictive analytics. In the *perceptual computing paradigm*, models/algorithms attempt to match incoming digital inputs (and engage associated cognition) with previously labelled digital categories. Predictive models may then be employed,

[15] Diagram by T. Butler.

in the form of 'if A, then B'. One use case could be facial recognition or biometric models (e.g. that carry out risk assessments for insurance purposes). Families of machine-learning, natural language processing algorithms and artificial neural network models currently perform these functions.

There are three approaches to designing and applying ML algorithms: supervised learning, unsupervised learning and reinforcement learning. In the first, subject matter experts classify concepts in the data and indicate the expected result, an algorithm is chosen from among several of the ML approaches including regression (statistical models), support vector machines, graph theory, Bayesian (Bayesian Belief Network — BBN; General Bayesian Network — GBN) or decision trees. A model results and this is used in concert with an algorithm when the machine is presented with new data to make predictions or recommendations. Thus, 'Supervised learning occurs when an algorithm learns from example data and associated target responses that can consist of numeric values or string labels, such as classes or tags, in order to later predict the correct response when posed with new examples'.[16] In the second, unsupervised learning, an algorithm learns how to classify data according to similarities. This approach is used to provide business, compliance and risk subject matter experts with insights into the meaning of specific data. Thus, the focus of this approach is primarily descriptive, however, they enable DL/ANN to help automate decision processes based on digital pattern matching. Unsupervised learning is also used in tandem with supervised machine learning algorithms. In the third approach, reinforcement learning refers to the use of goal-oriented algorithms, which learn how to attain a complex objective or maximize the value of outcomes along a particular dimension over several stages. This type of learning involves positive or negative reinforcement of algorithm behaviour through rewards for correct behaviour towards a desired objective or outcome. Reinforcement algorithms are designed to operate in a specific environment and make decisions in a stepwise fashion over time under a particular policy. There will typically be a delay between action and response, with positive or negative rewards from the environment, depending on its state, acting to nudge the algorithm to achieve a long-term value, as opposed to the short-term reinforcement reward. Examples of reinforcement learning include portfolio management and fraud prevention.

As AI technologies mature, so too will the degree of automation and information being provided to financial institutions, market participants and consumers. Examples of the application of AI in the financial industry include the following use cases:

- Robotic Process Automation for front, middle and back-office automation, including authentication;
- Risk alerts and compliance monitoring;
- Automated speech and writing;
- Descriptive analytics for regulation summarisation;
- Predictive analytics for investment modelling and to assess insurance risk;
- Diagnostic Analytics for fraud detection;

[16] Mueller, J. P. and Massaron, L. (2016) *'Machine learning for dummies'*, John Wiley & Sons, Hoboken, NJ.

- Prescriptive Analytics to assess credit and risk underwriting;
- RoboAdvice regarding products and services in the form of Chatbots and Virtual Assistants;
- Digital Process Automation.

Despite the wide range of applications as indicated in the following heatmap, the impact is still limited. According to an industry representative quoted in the press "*there are too many people making these statements [about big cost and job impacts]…The problems we have solved are very narrow. The misconception is that humans and machines can perform at the same level. There's still a long way to go and many challenges we need to solve before a machine can operate [at a level] even near the human mind.*"[17]

| Business Objectives | Risk assessment and scoring | Security Fraud Detection AML Risk Alerts Compliance | Regulation Summary Automatic reporting | Front, Middle, & Back Office efficiency Communication automation | Customer Profiling Customer Advice and marketing New CRM | Markets and Investment banking |
|---|---|---|---|---|---|---|
| AI Technology | Legend: Widespread Use | | Frequent Use | | Infrequent Use | |
| Robotic Process Automation | | | | | | |
| Descriptive Analytics (e.g. regressions, GAM, GLM, etc.) | | | | | | |
| Predictive Analytics (Time series and Forecasting models) | | | | | | |
| Diagnostic Analytics (e.g. Graph Analytics) | | | | | | |
| Prescriptive Analytics (Recommendation algorithms) | | | | | | |
| Robo Advice (NLP-enabled Chatbots) | | | | | | |
| Digital Process Automation (Image recognition, OCR, NLP) | | | | | | |

**Figure 2 AI Use Case Heatmap**

[17] Noonan, L. (2018) *AI in banking: the reality behind the hype, The industry is taking a cautious approach in spite of excitement about new technology,* Financial Times, London April, 12, 2018, https://www.ft.com/content/b497a134-2d21-11e8-a34a-7e7563b0b0f4. to F. Agrafioti, head of Royal Bank of Canada's AI research arm Borealis, in a statement to the Financial Times

The Group concludes that AI will realise its full potential when knowledge representation, machine learning, deep learning and natural language processing are employed in concert. This integrative approach should help minimise the risks associated with the current approach of using 'black box' machine learning and deep learning, which results in outcomes – e.g. client on-boarding or investment recommendations that cannot be explained, by either machine or human. Explainable AI technologies will therefore be required.[18]

## *Blockchain/Distributed Ledger Technologies*

Blockchain and DLT store tamper-proof, timestamped transactions or records on a distributed data store. These distributed data stores are shared public or private records of transactions among parties in a process or transaction. While there is a formal distinction between blockchain and DLT, it should be noted the terms are often used interchangeably in common parlance, and their characteristics continue to evolve as the technology develops.

This core digital technology's disruptive capability is that it allows parties to transact with trust over a computer network in which nobody is trusted. Take, for example, that blockchain /DLT applications can be used to track the lifecycle of a financial transaction between counterparties, without a trusted intermediary; to create secure financial products; and to deliver trusted and technologically sophisticated financial services. The technology is in particular envisaged for payments, trading and trade finance, regulatory reporting, digital identity, credit scoring and customer loyalty programmes.

Blockchain and DLT use as enabling technologies notably peer-to-peer networks, consensus-making algorithms, and cryptography. A Blockchain/DLT network has four essential characteristics: *shared record keeping, multi-party consensus, independent validation, tamper evidence and resistance*[19].All this makes Blockchain/DLT an ideal platform for all kinds of assets or entitlements, so-called crypto-assets. Blockchain/DLT are also ideal for managing the ownership and lifecycle of analogue assets whether fixed (e.g. buildings to works of art) or mobile (e.g. products shipped through supply chains).

Despite there being several important distinctions between blockchain and DLT, the latter has become an umbrella term to designate multi-party systems that operate in a secure environment with no central operator or authority in place, but which mitigates the risks posed by parties who may be unreliable or malicious ('adversarial environment'). Blockchain technology is a

[18] Butler T. and O'Brien, L. (2019). *Artificial Intelligence for Regulatory Compliance: Are We There Yet*? Journal of Financial Compliance, 3(1), 1-16.

[19] Rauchs, M., Blandin A., Bear, K., McKeon, S. (2019) *2ND Global Enterprise Blockchain Benchmarking Study*. The Cambridge Centre for Alternative Finance (CCAF), University of Cambridge Judge Business School.

specific subset of the broader DLT universe that uses a particular data structure consisting of a chain of hash-linked blocks of data.[20]

## *Blockchain explained*

The term blockchain[21] arises from the fact that the technology's data architecture is based on a chained list of data blocks distributed over a decentralized peer-to-peer computer network, in which every network node maintains the latest version of the chain of blocks. Processing of transactions and the creation of blocks are carried out by this distributed network of computers. Blocks contain data about transactions or can contain chain code. This allows, for example, recording and execution of transactions between an investment bank and asset managers, or institutional investors etc. Related DLT implementations work in a similar fashion, but non-blockchain-DLTs do not suffer the limitations of pure blockchain approaches and may therefore be more suited for digital business transformation.

When a new block is added to the blockchain, it is timestamped, a pointer to the previous block in the chain provided, and the transaction data entered. It is then processed by the cryptographic technique of *hashing*. A hash is calculated on the hash of the previous block plus the data contents of the new block. The result then becomes the hash of the new block. If a single bit in the chain is changed, through hacking or other fraudulent activity, then the hash value will no longer represent the data values in the blockchain. An audit could then discover which block has been corrupted. Thus, the security and trustworthiness of the data is ensured.

In addition, the hash in each new block in a chain is digitally signed using public/private key encryption, as also used for everyday Internet secure data transfers, to ensure strong authentication, data encryption and digital signatures. A hash signed with a private key can be decrypted only by using the corresponding public key—both have a unique mathematical relationship, and it is this that provides public key cryptography with its utility. In the blockchain scenario, the hash validates the integrity of the added data, while the digital signature (encrypted hash) validates that the data is authentic. Together they ensure strong security.

One further technical point of merit. A blockchain entry is immutable, and blocks, nor the transactions therein can be deleted or modified, because of the way the technology works. Situations may arise, particularly where data privacy is concerned, where personal data cannot be deleted, without invalidating an entire blockchain. Despite this, there exist many implementation alternatives for solving this issue such as: persisting data externally or implementing encryption. This is commonly cited as a major disadvantage of a pure blockchain

[20] Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., ... & Zhang, B. Z. (2018). *Distributed ledger technology systems: a conceptual framework.* The Cambridge Centre for Alternative Finance (CCAF), University of Cambridge Judge Business School.

[21] A detailed explanation of blockchain technology is outside the scope of this report, see Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *Blockchain technology overview*. National Institute of Standards and Technology (NIST) arXiv preprint arXiv:1906.11078.

approach; however, as the technology evolves there are a growing number of ways to solve for or work around this perceived limitation.

## *How DLT and Blockchain relate to each other*

As with blockchain, the objective of a DLT is to produce and maintain valid, authoritative records using a multi-party consensus process, in which multiple separate legal entities collaborate without the help of intermediaries, such as central authorities.

DLT networks can be public and permissionless as observered in most cryptocurrencies, or private and permissioned, as observed in private industry use cases where goverance of the network is centrally controlled. Unlike many public permissionless blockchain networks, it is possible for records stored on a DLT system to not be immutable and thus updated ordeleted. This allowsdifferent degrees of transaction finality to be possible, depending on the concrete DLT design and rules established by the network's participants. Private permissioned DLT networks can therefore achieve many of the benefits of blockchain, without requiring work-arounds for commonly cited limitations, such as GDPR compliance or high energy usage seen in a subset of public blockchains.

Finally, DLT networks can tolerate, with respect to the processing and recording of data, the existence of honest unreliable or dishonest fraudulent actors. However, they require trust among the parties.

## *Smart Contracts*

The term 'smart contract' refers to computer code that is designed automatically to execute programmatically-defined contractual duties upon the occurrence of a trigger event. Originally, the term referred to arrangements the automatic execution of which is truly unstoppable. However, in practice, the term refers often to arrangements of automated execution generally, even if some parts of the process may require human input and control. Further, there is little clarity as to the question of whether it is just "a computerized transaction protocol that executes the terms of a contract, or whether the smart contract itself has binding force between the parties."[22] Generally, smart contracts are thus viewed as efficient approaches for automating some of the conditions and obligations described in a legal contract. However, emerging

[22] See Tapscott, Don; Tapscott, Alex (May 2016). *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World.* pp. 72, 83, 101, 127; P. Paech, *The Governance of Blockchain Financial Networks,* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875487 p. 1082. C. D. Clack, V. A. Bakshi, and L. Braine, "*Smart Contract Templates: essential requirements and design options,"* ArXiv e-prints, Dec. 2016; ISBN 978-0670069972.

technology focuses on smart legal contracts that blur the distinction between contractual conditions embedded in code and embedded in legal contracts.[23]

While smart contracts were originally a self-standing concept that predated blockchain, they unleash their full potential, in particular when run on blockchain or DLT networks, because the latter offers the necessary certainty of execution.[24] As they are protected by the authentication and security measures described above, they are trusted mechanisms to implement legal, business and regulatory rules. The trusted automation of legal contract execution by smart contracts, combined with the immutability of transactions on a blockchain, renders this combination a truly innovative, disruptive technology. They support a range of new business models as well as the automation of existing models.

Zero-knowledge proof, or zero-knowledge protocol, will enhance the use of blockchain and DLT, including smart contracts.[25] ZKP is a method by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x. The essence of zero-knowledge proofs is that it is possible to prove the possession of information or knowledge without revealing the information itself. This has significant implications for identity management, authentication, and other cryptographic problems. It has major implications for the financial industry, not only in digital identity and cybersecurity, but also for blockchain/DLT, as indicated.

Smart contracts can be used in finance in the following contexts:

- Loans and financing: validating transactions, verifying the legitimacy of counterparties, and performing routine account administration.
- Mortgages: a single platform to integrate the activities of all agents: lawyers, realtors/estate agents, appraisers, bankers, mortgage brokers, engineers, home buyers and sellers. Again validating transactions, verifying the legitimacy of counterparties, and performing settlement.
- OTC (over-the-counter) trading of currencies (inc. crypto), commodities, and securities.
- Derivative trading: matching traders, validating transactions, verifying the legitimacy of counterparties, holding counterparty funds and contract settlement. Crypto-assets of derivatives such as futures contracts, forward contracts, options, swaps, and warrants.
- Derivatives Markets: centralized and de-centralized exchanges could emerge.
- Insurance policies: managing claims in a responsive and transparent way, through KYC and accurate risk evaluation, lowing administration and underwriting costs, accurate pricing, automated claims submission and processing, improved claims assessment and

[23] P. Paech, *The Governance of Blockchain Financial Networks*, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875487* p. 1100.

[24] Butler T., Al Khalil, F., O'Brien, L. and Ceci, M. (2017). *Smart Contracts and Distributed Ledger Technologies in Financial Services: Keeping Lawyers in the Loop*. Banking & Financial Services Policy Report, 36 (9), 1-11.

[25]Smart contracts were shown to be possible in 1985 by Shafi Goldwasser, Silvio Micali, and Charles Rackoff in the paper *The Knowledge Complexity of Interactive Proof-Systems.* https://en.wikipedia.org/wiki/Zero-knowledge_proof

costing, fraud detection, and automatic payments. Again all agents and parties to a claim use one platform increasing transparency, integrity and so on.

- B2C: recording digital assets transactions or exchanges.
- B2B: implementing complex payments for asset/payment transactions.
- Regulatory reporting: the combination of smart contracts and blockchain could help better automate and make more efficient and transparent regulatory reporting on financial compliance and risk.[26]

## *Quantum computing*

Quantum computing will have a profound effect on society and current computational systems, from AI to Blockchain, from secure digital payments to High Frequency Trading (HFT). However, it will neither render obsolete nor replace extant classical computer systems, which remain adequate for the vast majority of computational tasks. The benefits of quantum computing include faster computation over highly complex problems, which may be intractable for traditional computer platforms and applications due to the need for massive computing power or where solving problems involves a high degree of uncertainty and incomplete knowledge. Current examples of intractability in computing problems, and obstacles to innovation include certain applications of machine learning (e.g. deep learning), cryptography, chemistry and biology (i.e. new medicines), among others.

The designs of traditional or classical computing architectures are based on Boolean logical operations on binary inputs (in terms of 1s/0s, true/false, on/off) that produce predictable binary outputs. The core hardware components are logic gates that perform arithmetic and logical operations under the control of software algorithms. Together this hardware-software combination produces specific data outputs for specific data inputs. These values are used to represent discrete or continuous analogue variables at the input and output. The problem with traditional approaches is scale. The greater the computing task, the more powerful (and in terms of size, bigger, e.g. more logic gates, memory and speed of operation) the hardware platform has to be. Distributed or grid computing are horizontal solutions to overcome the vertical scaling problem with individual computers.

Quantum computing involves a fundamental change to classic hardware architecture and software design and practice. Quantum computers represent information using quantum bits (qubits) which are not classical mutually exclusive 1s or 0s, with states of on or off. A quantum state represents the unknown properties of an object at a point in time, before the state of the object becomes known. This is called a *superposition*. The ultimate value of a *superposition* depends typically on the status of other objects. The mathematical relationships between the object in question and related objects are unknown at the time of compute, thus the value of a

[26] https://www.fca.org.uk/publication/discussion/digital-regulatory-reporting-pilot-phase-1-report.pdf

*superposition* is both 1 and 0, that is both on and off. Thus, unlike a classical logic gate, a quantum gate has as its input several *superposition*s and it produces a determined state as its output, once the probabilities of the accuracy of the final position have been resolved.

Quantum computing architectures are based on quantum mechanics and quantum logic (as opposed to Boolean Logic) and involve the application of rules, based on the principles of quantum theory, in order to reason about propositions that deal with the solution to complex problems of great uncertainty. Quantum reasoning is based on complex mathematics which are integrated into algorithms and when executed using quantum gates help solve highly complex intractable problems that are beyond the power of classical computing architectures. Quantum machines also perform complex problem-solving in far less time than traditional architectures.

Thus, the advent of quantum computing may negatively impact and make obsolete the existing cryptographic systems on which the financial industry relies heavily. Current cryptographic algorithms are industry standard and employed in digital certificates, message encryption, authentication and even physical authentication devices in the Internet of Things. Some argue that the financial industry is as unprepared for the consequences of quantum computing, as it is for the next global financial disaster. Finally, if used to enhance HFT, quantum computing may lead to even higher levels of systemic risk, or it may mitigate existing risks if used wisely. Regulators need to be aware of and take appropriate action in advance of such solutions coming to market.

## *Internet of Things: enhanced consumer data and transactions*

Simple examples of Internet of Things (IoT) use cases are where a smartphone or smartwatch can made debit cards redundant, or where retail banks might mimic the way retailers are already starting to place sensors in stores to suggest product details, discounts and recommendations through the consumers' smartphones.[27] Recent research shows that consumers who receive personalized messages are nearly 20 times more likely to buy. By connecting retail banking systems straight through to customers' personal systems, banks might increase cross-selling opportunities and enhanced services with personalised messages.

In the insurance sector, IoT used in wearables or telematics in vehicles can provide enhanced risk data profiles on customers. For example, some car insurers can access drivers' behaviour data so that they can assess drivers' risks and adjust premiums accordingly. This may benefit low-risk drivers whose premiums will fall as a result of their safe driving behaviours, however this could lead to a race to the bottom, where those with the lowest risk are the only ones able to source economically viable policies. IoT-enabled smart home platforms will be able to provide data about how homes and apartments are managed, with insurers rewarding low-risk behaviour. With the growth of the IoT and 'smart homes', all such data can now be collected,

[27] Lande, R. S., Meshram, S. A., & Deshmukh, P. P. (2018, August). *Smart banking using IoT*. In 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE) (pp. 1-4). IEEE.

managed and shared.[28] However there are increasing risks regarding the security* of these devices and regulation should consider how the implementation and manufacture of IoT devices and networks are overseen to protect threats to broader infrastructure and services. In the future if such devices are able to act on behalf of consumers when facilitating payments or making decisions, then the security of these devices and the ability to identify risk actors is essential to maintaining the stability and trust of financial services.

[28] https://www.mckinsey.com/industries/financial-services/our-insights/digital-ecosystems-for-insurers-opportunities-through-the-internet-of-things

# Recommendations and Background

# Innovative use of technology in finance

EU financial services legislation should be technologically neutral, sufficiently future-proof, and fit-for-purpose. Indeed, regulation should be designed to adequately capture any way in which technologies are currently, or will in the future be, used to provide financial services. However, in terms of regulatory approach, it would be inefficient to conceive a framework that was tailor-made for just one specific technology: a 'Blockchain/DLT regulation', for instance, would not make much sense, as it would be incapable of capturing the constantly evolving possibilities and uses of technology. A more efficient approach is to identify those themes that are *common* to all technologies employed in the provision of financial services, and to conceive regulatory strategies in response to those common themes. The Group has identified five such themes: understanding technology and its impact, cyber resilience, outsourcing, Governance of distributed financial networks (including the legal framework for crypto-assets), and standardisation, RegTech and SupTech.

## *Understanding technology and its impact*

***<u>Recommendation 1 – Explainability and interpretability of AI and associated technologies</u>***

***The Commission should, in co-operation with the ESAs and relevant international standard-setting bodies:***

- ***develop measures clarifying the circumstances under which requirements aiming at explainability or interpretability of AI and associated technologies, in their concrete applications, are appropriate, considering the need for sector-specific or horizontal rules;***
- ***provide guidance on how to meet explainability and interpretability requirements, where applicable, in respect of different stakeholders, including consumers and supervisors, acknowledging that different standards will be needed depending on the type of application for which the relevant technology is being used.***

*Background*

AI, Big Data and machine-learning solutions are being increasingly applied in the financial sector, for instance in the context of automated brokerage and investment management, insurance underwriting pricing and claims management, and credit scoring (see relevant use

cases, below[29]). Indeed, the increasing use of AI has caused the European Commission to establish a High Level Expert Group to consider the application of AI and the relevant consequences.[30]

Precisely how AI functions influences the outcomes of the processes in which it is used. From the outset, only the actual designers of the relevant device or the programmers of the relevant algorithm possess a deep understanding of its functioning. However, even for them and other specialists, it may either not be possible or else very difficult to accurately understand and explain the outputs generated when using the different forms of AI, such as machine-learning models using neural networks and deep learning algorithms, which are also sometimes referred to as "black-box" algorithms.

> ***Use case: Automated brokerage and investment management***
>
> *Automated brokerage and investment management, often referred to as 'robo-advice', offers customized investment or related services that, within a certain risk profile, use algorithms of varying sophistication to assess the client's needs and risk profile and to analyse the relevant markets, with the aim of investing across a portfolio of assets on behalf of clients.*
>
> *Automated brokerage applications can improve consumer choice for investment products by broadening access to investment products and reducing costs. They can also enable portfolio optimisation and rebalancing, potentially improving long term returns.*
>
> *The fact that the core function of the advice process is powered by AI, at the same time, creates risks very similar to the principal agent problem traditionally inherent in investment advice. Whereas traditional causes for suboptimal investment advice are probably easier to address in an automated environment, clients provided with automated advice face the difficulty that it is virtually impossible to review the processes and parameters that inform the relevant investment absent higher standards of explainability.*

It is accepted that models using such algorithms provide very accurate predictions. However, the subjects of such decisions, consumers and businesses alike, may face situations in which they have no real possibility to assess the correctness or appropriateness of the relevant decision, depriving them of the option to challenge or appeal against it or have it reviewed by courts.[31]

Article 22(3) of the GDPR on automated decision-making requires data controllers to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express

[29] See, in addition, the European Banking Authority's (EBA) report on *Big Data and Advanced Analytics* (December 2019).

[30] European Commission, *Ethics Guidelines for Trustworthy AI* (2019) <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top > accessed 6 November 2019.

[31] Philip Alston, *Extreme poverty and human rights* (2019) < http://www.statewatch.org/news/2019/nov/un-report-digital-welfare-states-10-19.pdf> | Accessed 6 November 2019

his or her point of view and to contest the decision. Those measures should include the provision of specific information to the data subject and in particular an explanation of the decision reached, so the data subject is in a position to challenge the decision[32]. However, these safeguards provide only limited protection as long as the data subject is unable to develop an understanding of the relevant decision-making process, in particular where black-box algorithms are used.

The issue of explainability is to some extent addressed in Article 13 GDPR, which requires firms to inform their customers about the existence of automated decision-making processes, as well as to provide them with meaningful explanation regarding the logic involved and the significance and envisaged consequences of such processing, differentiating between different stakeholders, e.g. regulators or consumers. However, the protection provided by those safeguards can be seriously undermined should data controllers encounter difficulties in providing clear and sufficient explanations about the relevant decision-making process, in particular where unsupervised learning algorithms are used.

Moreover, firms may have no specific interest in revealing the precise functioning to their customers, counterparties or the market as a whole. They might consider this as part of their intellectual property or commercially sensitive information that could put them in a disadvantaged position vis-à-vis their competitors. Relevant disclosure practices at the national level are inconsistent due to divergent local requirements.[33] This may deter firms from seeking to provide services cross-border due to compliance costs and complexities stemming from these varying requirements.

At the same time, supervisors face challenges in assessing the risks posed by a certain practice (e.g. systemic risks, or concerns regarding consumer protection) and may, in view of this, be less open to the use of AI solutions in practice.

---

***Use case: Insurance products and services***

*AI, Big Data Analytics processes, and machine learning algorithms are increasingly applied in the insurance sector.*

*For example, technology-enabled underwriting and pricing is used to provide tailored insurance policies and the use of portfolio and single risk analytics, the technology enabling more granular segmentation of risks, a higher effectiveness of risk identification, thus allowing for pricing that is more risk-sensitive.*

*A further example relates to post-sales and assistance services, where firms increasingly use sophisticated Consumer Management Systems (CRM), robo-advisors and especially chatbots to interact with their customers. Firms also use the data collected through IoT devices to provide a wide*

---

[32] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], recital 71

[33] European Banking Authority, EBA report on *Potential Impediments to the Cross-Border Provision of Banking and Payment Services* (2019) <https://eba.europa.eu/eba-calls-european-commission-take-action-facilitate-scaling-cross-border-activity> | Accessed 6 November 2019

*range of risk mitigation services such as recommendations to improve driving skills or to adopt healthier lifestyle.*

*Lastly, Big Data Analytics are widely used on claims management, most often in enhanced fraud analytics, followed by automated payment processes, segmentation of claims and invoice verification. This includes so-called parametric insurance solutions, providing automatic payouts, for instance in the case of flight delay insurance or agricultural crop insurance, sometimes using DLT/blockchain, although such use is at present not yet common in the insurance context.*

---

The Group considers that it would be useful to clarify the supervisory expectations in this area. The concepts of explainability and interpretability should be elaborated, and it should be made clearer how the relevant obligations towards stakeholders should be calibrated, depending on the type of stakeholder (regulators, businesses, consumers) and the different contexts in which AI, Big Data and machine learning may be used. In particular, the ESAs should develop guidelines on the use of AI, Big Data, and machine learning solutions in the context of credit-scoring, reflecting current European Banking Authority (EBA) work on this issue and ensuring that these guidelines are applicable to any type of financial institution, including with a view to promoting high standards concerning outcomes and transparency towards consumers with respect to the general decision-making process. Transparency will help consumers understand the data used and criteria behind the decision, increasing their ability to take action in order to effect a different outcome, and, hence, will also build trust in the financial system.

In developing these standards it should be taken into account that all parties should be able to smoothly and easily handle the operationalisation of those standards. The provision of more detailed explanations should be required for use by supervisors (as compared to consumers), in particular relating to those processes or models which potentially have a significant impact on financial stability or consumer protection, for instance, concerns regarding unfair discrimination or financial exclusion (see also Recommendation 29). Further, different standards should apply depending on the concrete application for which the relevant technology is used. It may be at the heart of customer-facing activity, such as sales and services, or, it may be used in the context of preventive or defensive internal applications, for example in the context of AML-related monitoring or cyber security.

***Recommendation 2 – Firms' internal IT governance***

***The Commission should, in cooperation with the ESAs, require regulated entities to build adequate levels of IT governance and technological expertise at the appropriate management level, including, where appropriate, at board level.***

*Background*

Some market participants that use relevant technology may lack sufficient knowledge about its opportunities, risks and functions, in particular as the commoditisation of the different IT tools by third-party service providers (e.g. cloud computing service providers cross-selling machine

learning solutions to their customers[34]) make them increasingly accessible to non-specialised users.

Our Group considers it essential for a well-functioning financial market that technology is truly understood by key players. As with regulation regarding risk management functions, expertise regarding the functioning of technology and appropriate internal controls should be required at appropriate management levels of a market participant (which might, where appropriate, also include board level) to make sure that technology-related questions are considered as a part of decision-making at all relevant levels.

Determining what is 'adequate' expertise, and at which level of management, will depend on the complexities, purposes and structures of the technologies applied, considering in particular the need for operational resilience, financial inclusion and consumer protection.

***Recommendation 3 – Supervisors' understanding of technology***

***The ESAs should be given a mandate to encourage and support supervisors in developing appropriate internal understanding, at appropriate levels, of the use of technology in financial services and the potential associated risks and opportunities.***

*Background*

As for other technologies, supervisors face challenges to keep pace with the industry in terms of knowledge and understanding of AI, Big Data, machine learning and DLT/blockchain solutions and their application in the financial sector. Supervisors may not necessarily have the level of expertise required to comprehensively assess whether an innovative solution should be permitted, whether to respond with appropriate guidance or rules setting out clear expectations, for instance in terms of auditability, explainability, governance and operational resilience, or how to challenge firms consistently and effectively in the course of day-to-day supervision.

For these reasons, supervisors have developed innovation facilitator initiatives to help enhance monitoring and engagement with industry on innovation related issues, and the ESAs are taking steps to promote more in-depth and common understanding of new technologies, for instance via the European Forum for Innovation Facilitators (EFIF)[35] and the EBA's FinTech Knowledge Hub.[36]

Notwithstanding these initiatives, currently, there are inconsistencies in the supervisory approach to risk management in relation to the use of AI, machine learning, Big Data and DLT/Blockchain (e.g. operational risk). These are impacting the acceptability and use of these technologies across the EU. In turn, in the absence of a clear EU-wide framework, regulated

[34] E.g. the IT provider IBM is one of the principal cloud service providers while at the same time offering "Customer Insight for Banking" powered by the Watson super computer.

[35] https://esas-joint-committee.europa.eu/Pages/Activities/EFIF/European-Forum-for-Innovation-Facilitators.aspx

[36] https://eba.europa.eu/financial-innovation-and-fintech/fintech-knowledge-hub.

entities currently lack a clear understanding of supervisory expectations regarding the application of technologies and, even where expectations have been set out clearly, these may vary from one jurisdiction to another.

To address these issues, there is a need for supervisors to equip themselves with adequate human and economic resources so as to ensure they possess up-to-date understanding of the different technological developments in the markets. They need to be able to assess available information on the functioning of technology, and to understand the risks and opportunities that flow from it. This extends, amongst other things, to the monitoring of whether herding effects associated with outcomes produced by AI applications might occur. For example, there may be a risk that strategies developed by competing algorithms and by different providers might lead to investment concentrations, for instance in ETFs, that increase volatility of financial markets in the event of market stress. It is important that supervisors approach technological developments from a multidisciplinary perspective, e.g. by employing experts with different backgrounds, including specialists on technological issues.

It is also important that supervisors engage in a proactive and continuous dialogue with stakeholders on technologies such as AI, Big Data and machine learning. The EFIF and the Global Financial Innovation Network (GFIN) provide useful fora for this purpose.

To promote a fully consistent (including cross-sectoral) supervisory culture and practice between supervisors, the ESAs should be mandated to support supervisors in capacity-building on technology-related issues.

## *Cyber Resilience*

### ***Recommendation 4 – Cyber resilience***

***The Commission should, in cooperation with the ESAs and the ESCB, develop a coherent and proportionate cyber resilience testing framework for the financial sector.***

*Background*

Financial institutions are increasingly switching to digital solutions to provide financial services. As a natural consequence, cyber threat levels are growing.[37] In response, supervisors and regulators are responding, for example the ECB, as overseer of financial market infrastructures, sets rules and best practices with the aim of ensuring that these infrastructures have a high level of cyber resilience.

[37] Joint advice of the European Supervisory Authorities on the *Costs and Benefits of Developing a Coherent Cyber Resilience Testing Framework for Significant Market Participants and Infrastructures within the whole EU Financial Sector* (2019) <https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/d229589f-a855-45f2-ad5a-411792792e60/JC%202019%2025%20(Joint%20ESAs%20Advice%20on%20a%20coherent%20cyber%20resilience%20testing%20framework).pdf > | Accessed 6 November 2019

In view of the borderless nature of cyber threats (both geographically and sectorally), consistent regulatory and supervisory requirements and expectations are needed. This is necessary, not only to ensure effective cyber risk mitigation, but also to protect the level playing field and to capitalise on cooperation and synchronisation in response to cyber risks.

For these reasons, the Group recommends that the European Commission takes action to develop a cyber-resilience testing framework for the EU financial sector. This framework should be coherent and proportionate in the sense that it should:

- provide guidelines and principles to supervisors in order to promote an EU-wide understanding of good practice;
- not cause disproportionate cost and burden to firms, as a result of testing or observations reported after testing, in particular taking into account their size and importance for the market;
- takes into account risks identified in the context of information security testing.

As a complement to measures to enhance cyber resilience, consideration should be given to the role of a well-functioning cyber insurance market.

## *Outsourcing*

***Recommendation 5 – Outsourcing guidelines and certification/licensing***

***The Commission, in cooperation with the ESAs and the ESCB, international standard-setting bodies and other relevant authorities, should regularly monitor the extent and structure of outsourcing of critical services by financial institutions, and assess the appropriateness of tools in place to mitigate concentration risks, operational risks and systemic risk, taking account of the potential impact on innovation and competition. On this basis:***

- ***the ESAs should regularly review the outsourcing guidelines with a view to maintaining their proportionality in light of technological developments, new risks and new market conditions;***
- ***the Commission, in cooperation with the ESAs, should consider the need to introduce a certification or licensing regime for third parties providing technology services to regulated entities.***

*Background*

Outsourcing allows firms to improve efficiency and to obtain ready access to technologies and business models. Outsourcing can be used to perform activities that form part of the value chain itself (such as client interaction, pricing, credit scoring, insurance claims management and

auxiliary services). It can also be used to buy in 'just' the technology and infrastructure, i.e. the digital solution that the outsourcer intends to use while performing itself an activity that is part of the value chain.

Outsourcing is regulated in the EU at different levels. For insurance companies, it is addressed in Article 49 Solvency II Directive, and Article 274 of Commission Delegated Regulation (EU) 2015/35. EIOPA is currently in the process of finalising guidelines for cloud computing outsourcing, which will provide guidance to insurance undertakings on how the outsourcing provisions need to be applied in the case of outsourcing to cloud service providers.[38] For banks, Directive 2013/36/EU (the CRD) strengthens the governance requirements for institutions and Article 74(3) CRD mandates the EBA to develop guidelines on institutions' governance arrangements, including outsourcing. In February 2019, the EBA issued revised guidelines on outsourcing arrangements, which integrate the earlier EBA recommendation on outsourcing to the cloud, taking account of the evolution in outsourcing practices particularly in light of the increasing use of technological solutions provided by third parties.[39] Directive 2014/65/EU (MiFID II) also contains explicit provisions regarding the outsourcing of functions in the field of investment services and activities, as does Directive 2015/2366/EU (PSD2) in relation to the outsourcing of functions by payment institutions. Directive 2015/849/EU (5th Anti-Money Laundering Directive) regulates "performance by third parties" upon whom obliged entities are entitled to rely when performing customer due diligence, while making clear that the ultimate responsibility remains with the obliged entity. In the context of securities depositories, there are legal requirements for CSDs on outsourcing (Article 30 CSDR). Where outsourcing involves critical service providers to payment systems, Eurosystem rules also apply, setting out specific oversight expectations for these providers in terms of risk identification and management, information security management, reliability and resilience, effective technology planning, and communications with users.

These rules ensure sound governance arrangements for outsourced services, as they are essential to protect the operational resilience of financial institutions and, in turn to mitigate risks to consumers and other customers resulting from, for example, system failures resulting in unavailability of essential banking services, data theft or data corruption.

However, outsourcing is becoming increasingly complex as a regulatory theme[40], as:

- financial institutions are increasingly relying on technology start-ups, BigTech and other important technology providers (e.g. regarding cloud services) to develop specific areas of the value chain, as this is often the fastest way to access relevant expertise and infrastructure. The underlying arrangements can differ and are often organised on the basis of an outsourcing relationship. As a consequence, financial institutions are

[38] European Insurance and Occupational Pensions Authority, *EIOPA Consults on guidelines on outsourcing to cloud service providers* (2019) <https://eiopa.europa.eu/Pages/News/EIOPA-consults-on-guidelines-on-outsourcing-to-cloud-service-providers.aspx> | Accessed 6 November 2019

[39] European Banking Authority, *EBA Guidelines on outsourcing arrangements* (2019) <https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf > | Accessed 6 November 2019

[40] For further discussion, see ibid

becoming increasingly dependent on outsourcees for strategic services and technologies;

- some outsourcing markets have an oligopolistic structure, as the relevant strategic services and technologies are becoming increasingly dominated by a handful of market players. This causes concentration risks, as the deep interconnectedness between a handful of critical service providers with the entirety of the financial system could create single points of failure;[41]
- the oligopolistic structure of the market combined with the technological dependency of regulated financial institutions on their service providers ('reverse outsourcing') may reverse the traditional power relationship between principal (the outsourcing financial institution) and agent (the service provider), leading to a situation in which the terms of their relationship are dictated by the latter, which is regularly an actor outside the perimeter of financial regulation;[42]
- this situation may be further complicated by the fact that some of the providers, notably BigTechs, are now entering the financial market themselves.

In light of these developments, it is essential that practices and market structure are continuously monitored and, where necessary, prompt action taken to mitigate any new risks. Concentration on a very limited number of providers should therefore be at the core of future monitoring of the situation, in addition to the traditional concern of operational risk, as both in combination may entail considerable systemic consequences.

It may also be necessary to consider measures beyond simply revising existing governance and outsourcing requirements. In particular, the Commission, in co-operation with the ESAs, should consider the introduction of a binding cross-border framework for third party service providers, notably in the form of certification or licencing regimes. Such a framework could also ensure appropriate cross-sectoral risk management, as the relevant third parties typically provide similar technology solutions to firms outside the financial sector and a new framework could allow for more effective oversight as compared to sector-based solutions. In developing this framework, the Group observes that the following elements should be recalled:

- a distinction should be made between, on the one hand, intra-group outsourcing and IPS-related network outsourcing, e.g. the distribution of data and processes across several entities of the group, which may entail lower compliance and reporting obligations, and, on the other hand, third-party outsourcing;

---

[41] *Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to the ICT risk management requirements in the EU financial sector* (2019) <https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/4d2ad5e2-1570-48bd-819a-7cd9b4e8b157/JC%202019%2026%20(Joint%20ESAs%20Advice%20on%20ICT%20legislative%20improvements).pdf> | Accessed 6 November 2019, which recommends the establishment of an oversight framework for monitoring the activities of critical third party providers in the context of ICT services.

[42] ESAs, ibid

- excessively burdensome or unclear certification or licensing requirements for third parties (e.g. on how to develop key governance processes such as materiality assessments) could limit the involvement of those parties in the value chain and therefore represent a barrier to financial innovation, impacting the competitiveness of the financial sector;
- a lack of competition in the availability of strategic services or technologies or at the distribution channel level could disrupt the efficient functioning of value chains, exacerbating issues associated with reverse outsourcing. This may result in a potential entry barrier for smaller firms, as they may not be able to access innovative financial technologies;
- licensing regimes offer the advantage of direct supervision, enabling a more holistic oversight of governance and risk-management, potentially over a range of business activities that may directly or indirectly impact services provided to financial institutions;
- certification regimes represent a less intrusive, and potentially lower cost means to help address operational resilience issues, however certification regimes may not be able to absolve the outsourcing financial institution of performing the necessary due diligence.

### *Governance of distributed financial networks; legal framework for crypto-assets*

DLT/Blockchain is a database technology which can have innumerable uses, e.g. in healthcare or supply chain management, and which *per se* does not need to be regulated. However, where financial market participants use this technology to execute functions that are relevant from the perspective of financial regulation and supervision, it needs to be ensured that such regulation applies without ambiguity. General regulatory concerns regarding distributed financial networks are addressed in Recommendation 7.

The function of a distributed financial network can have just an informational character, or can be combined with other technologies, for instance for the recording and administering of so-called 'crypto-assets' (or 'digital assets', 'tokens', 'coins', etc. – the terminology is inconsistently used). Crypto-assets are entitlements enshrined in a piece of computer code. At the moment, they are typically stored on distributed financial networks (see use case below). However, that is not a necessary requirement. Crypto-assets, depending on their nature, might be clearly covered by existing regulation; in other cases, either the application of existing regulation is unclear or regulation does not apply. Issues regarding crypto-assets are addressed in Recommendation 8.

Complex questions in terms of commercial and insolvency law arise where crypto-assets are stored and transacted on a distributed financial network. Uncertainty in this respect may

undermine not only respective rights of market actors, but also negatively impact the functioning of collateral, risk management and regulatory capital mechanisms. This issue is addressed in Recommendation 9.

***Recommendation 6 – Distributed financial networks***

***The Commission, in co-operation with the ESAs, the ESCB and international standard-setting bodies and other relevant authorities, should take action to clarify the regulatory framework applicable to distributed financial networks, in particular to:***

- ***a. assess and clarify how relationships between participants should be regarded for regulatory and supervisory purposes, taking account of existing concepts such as agency and outsourcing;***
- ***b. ensure the applicability of defined terms and established concepts in existing regulation, such as SFD, FCD, CSDR, EMIR, MiFID, the SIPS Regulation or AMLD in view of the shift from bilateral relationships to a multilateral environment where functions can be attributed simultaneously to several parties;***
- ***c. define the addressee of relevant regulation concerning distributed financial networks;***
- ***d. assess and clarify how issues of operational resilience and higher exposure to cyber risks (in particular with regard to private key management) or systemic network failures, should be addressed.***

*Background*

*Clarifying the shift from bilateral to multilateral relationships*

The financial market is adopting practices built on increasing disintermediation and decentralisation of services, products and functions. Existing and emerging technologies, such as cloud, Blockchain and DLT are increasingly being adopted, piloted and deployed in the context of the delivery of financial products, services and functions. These technologies exhibit a number of distinctive features, as described earlier. One critical feature is their 'distributed' (or mutual) nature. As is the case with cloud solutions, data is distributed or replicated across different locations using mirror or replication approaches up to fully distributed data stores. DLT and blockchain data stores typically have their data distributed across data stores in public or private infrastructures, however, as opposed to cloud, identical data is stored in each place and each copy has on its own the same constitutive value.

The idea of 'distributed' delivery of services, products or functions in the financial market is to be distinguished from two other types of relationships currently underpinning the market for financial services, i.e. from outsourcing and from providing accounts, because:

- Distributed networks are different from typical outsourcing arrangements. In the outsourcing scenario, the service provider acts in structural subordination for the outsourcer. In the distributed settings, several parties mutually perform a function for

and to each other, notably, keeping a distributed record and verifying the validity of transactions. This distinction may be blurred where the participants in a decentralised network employ a service provider for certain central functions, or in a situation of an outsourcer entrusting a function to an outsourcee, who then uses a distributed network to perform this function;

- Decentralised networks are different from account relationships (which for present purposes is understood to include agency and custodian relationships) of the type that underlie today's financial market. An account is a two-party relationship. Accounts may be stacked or linked with each other, as is the case, for example, in securities settlement. However, even such a complex structure still consists of a combination of two-party relationships. Distributed networks do not contain any two-party relationships. They are truly multilateral.

The current legal and regulatory framework is built around the traditional bilateral understanding of outsourcing and account relationships as building blocks of the financial market. Wherever services, products or functions will in the future be delivered using a distributed setting (e.g. in asset settlement, payment, crypto-assets, etc.), the current legal and regulatory framework will not apply smoothly[43].

This extends to the problem of unclear legal recourse: users may be dealing with parties in jurisdictions from across the EU or around the globe and within complex set-ups. In the event of fraud, error, or insolvency, in a distributed setting it may be unclear whether a party will have legal recourse against any of these parties and which regulatory jurisdiction the customer and provider may fall into.

It is therefore important to build a common conceptual understanding regarding the transition from the present financial sector that is exclusively built on bilateral relationships, notably outsourcing and account relationships, to a financial sector which is, in addition, increasingly using multilateral relationships as established in distributed financial networks.

---

***Use case DLT: Infrastructure for trading, clearing and settlement of cash and financial instruments***

*The core activities of financial market infrastructures (FMIs), such as stock exchanges or clearing systems, comprise primary issuance, trading and settlement with finality of financial instruments and cash, as well as safekeeping. These activities necessitate permanent interfacing with markets, the development and maintenance of immense IT infrastructure, demanding the highest standards of cybersecurity, the development of technical standards and messaging protocols, measures pertaining to CDD and AML, sanctions screening, tax compliance, and supporting regulatory oversight.*

---

[43] Philipp Paech, *The governance of Blockchain financial networks* [2017] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875487.

*Emerging technologies, in particular DLT, may facilitate and enhance the efficiency of vital infrastructure functions, rendering the trading and post trading environment more competitive.*

*Incumbent FMIs increasingly recognise the potential of DLT and have become actively involved in their research, experimentation and development of DLT applications. In particular with a view to DLT's potential of alleviating the current – significant – reconciliation burden between financial market participants, that creates significant operation and legal cost.*

*In terms of developing new markets, FMIs tend to follow market dynamics in order to facilitate their growth. They are now participating in the development of markets for new asset classes, such as, in particular, crypto-assets. In terms of examples, infrastructures, together with custodians and large investment fund providers, have announced crypto-asset offerings.*

*FMIs operate in a regulatory environment shaped by MiFID/MiFIR, the Prospectus Regulation, UCITS, AIFMD, CSDR, SFD, PSD, FCD, AMLD, EMIR, the SIPS Regulation and other, more general EU and autonomous national rules. Bar a number of exceptions, such as so-called utility tokens, there seems to be no need for significant changes to existing regulation regarding FMIs to accommodate the application of new technologies in the sector. Rather, there is a need for clarification in the sense described above, with a view to avoiding uncertainty of application.*

*Ensure application of terms and concepts used in existing regulation*

For financial regulation to apply, the relevant DLT/blockchain network needs to fall within the regulatory perimeter. This is typically the case where regulated financial institutions, in the course of their business, make use of such a database for storing or sharing information, or for similar purposes. As a minimum, such networks are covered by rules regarding operational resilience. More complex regulation may apply, for example where such networks are used to log information or share it in compliance with specific regulatory requirements, such as under EMIR or MiFID. Further, and probably most visibly, use cases for distributed networks may fall within the scope of regulation as a consequence of the nature of the data stored, notably where this data represents a crypto-asset that is covered by existing regulation with respect to regulated products and services (financial instrument, e-money, etc.), as discussed under Recommendation 8, below.

Wherever an existing regulation, such as CSDR, EMIR, FCD, SFD, MiFID, the SIPS Regulation and AMLD, is engaged, defined terms and established concepts may not apply unambiguously. For instance, fundamental notions such as 'account', 'client', 'customer' need clarification as they are based on a 'bilateral view' of relationships which cannot be applied smoothly in the context of a DLT network. Concepts such as 'trade repository', which is an entity connected to the market through a large number of bilateral relationships, may need to be translated into the multilateral context of distributed financial networks, as would terms such as 'system', 'book entry', 'settlement', or 'finality'. Similarly, fundamental ideas of client asset protection or segregation are not translated easily into a distributed, multilateral environment.

The relevant questions will inevitably occur wherever market participants and supervisors attempt to use and supervise distributed financial networks under existing rules and any absence of clarity will restrict market participants' and supervisors' openness to this technology. In responding to these questions, it is important to ensure consistency and uniformity regarding the concrete applications of regulatory terms and concepts across the EU. Sectoral divergences, e.g. per relevant regulatory area, or approaches fragmented along jurisdictional borders, would gravely restrict the adoption of such networks across the EU.

*Defining the addressee of relevant regulation*

Distributed financial networks may or may not have an operator that provides central services for the entire network; they may or may not may have nodes that, collaboratively or collectively perform certain functions, whereas other nodes do not participate in this task. Additionally, networks may follow the logic of free, unrestricted and uncontrolled enrolment and participation of new members ('un-permissioned networks'), including potentially consumers or unregulated entities, or consumers or entities outside the reach of EU regulation. Especially, but not exclusively, in these three cases it may be unclear who should be the addressee of relevant financial (and other) regulation.[44] This problem is exacerbated by the fact that such networks use the Internet as the underlying infrastructure and in consequence participants may operate from anywhere around the globe – or may not even be identifiable. There are also other, less problematic cases, in particular those in which regulated financial institutions co-operate in closed networks.

*Operational resilience, especially private key management*

The increasing use of DLT/Blockchain technology may require that additional attention be afforded to questions of operational resilience and vulnerabilities to cyber risk. A concrete example relates to the management of private keys, necessary to access information stored in a database. The public/private key mechanism pre-dates DLT/Blockchain, however, in this context, it may become difficult, if not impossible, to retrieve data, including crypto-assets, should the private key be lost, as the concept of current DLT/Blockchain applications may be incompatible with the idea of a recourse for recovery of those assets. In the context of DLT/Blockchain, it is therefore vital to ensure the functioning and security of the public/private key mechanism, as there may be no remedies to mitigate the consequences of theft or loss of the private key.

Relevant best practices entail the use of certain specialised hardware devices that provide a nearly impenetrable layer of security for private keys. In applying these established best practices, theft and loss of data stored on DLT/Blockchain networks as a consequence of problems relating to the private key can be largely excluded.

However theft or loss of data stored on distributed financial networks, including crypto-assets, could still occur as a consequence of other points of failure, in particular if access is gained through the people and processes that authorise a specific transaction of transfer.

---

[44] Philipp Paech, *The governance of Blockchain financial networks* [2017] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875487.

For these reasons, it is important that common and robust standards of operational resilience, including, security standards, are in place.

***Recommendation 7 – Crypto-assets***

***The Commission, in co-operation with the ESAs, the ESCB and international standard-setting bodies and other relevant authorities should accelerate its work to assess the adequacy and suitability of existing rules mitigating risk flowing from the use of crypto-assets in the context of the provision of financial services and on this basis develop a legislative solution to complement and complete the framework where necessary. This process should extend to addressing:***

- ***a. the risk and uncertainty flowing from the lack of a common taxonomy in respect of crypto-assets and the consequential fragmented national approaches to classifying crypto-assets under EU rules, such as MiFID or the e-money Directive and emerging national law;***
- ***b. the risks flowing from activities involving crypto-assets, in particular, in relation to:***
  - ***money laundering, terrorist financing and tax evasion;***
  - ***governance and operational resilience;***
  - ***client asset protection, including regarding segregation of client assets, redemption rules, disclosure requirements, and consumers' interests;***
  - ***systemic effects, including through threats to the orderly functioning of the payment environment;***
  - ***the prudential treatment of regulated financial institutions' exposures to crypto-assets;***
  - ***pegging and foreign exchange conversion mechanisms.***

*Background*

*Taxonomy of crypto-assets*

There is no unique or precise definition of what crypto-assets are, and a variety of terms describe more or less overlapping phenomena (digital assets, tokens, ICOs, virtual currency, etc.)[45]. This

[45] European Banking Authority, *Report with advice for the European Commission on crypto-assets* (2019) < https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1> | Accessed 6 November 2019; European Securities and Markets Authority, *Licensing of FinTech business models* (2019) < https://www.esma.europa.eu/sites/default/files/library/esma50-164-2430_licensing_of_fintech.pdf> | Accessed 4 November 2019; European Securities and Markets Authority, Advice: *Initial Coin Offerings and Crypto-Assets* (2019) < https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> | Accessed 6 November 2019 - European Securities and Markets Authority, *Crypto-Assets: Time to deliver* (2019) <https://www.esma.europa.eu/sites/default/files/library/esma71-99-1120_maijoor_keynote_on_crypto-assets_-_time_to_deliver.pdf> | Accessed 3 November 2019; European Securities and Markets Authority, *Advice: Own Initiative Report on Initial Coin Offerings and Crypto-Assets* (2018) <https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf> | Accessed 4 November 2019;

report uses the term crypto-assets in a broad sense, to mean assets that are embodied in, represented or evidenced by pieces of unique digital code. Other descriptions are narrower. Regardless of which definition is retained, the understanding of what we are dealing with in regulatory terms is still varied. In the early years of the discussion (2008-2011), so-called 'virtual currencies' (e.g. Bitcoin) were the main incarnation of crypto-assets[46]. However the characteristics and uses of crypto-assets have evolved rapidly since. There are now more than 2,000 privately issued crypto-assets with different natures.[47]

Nor is there yet a common taxonomy of crypto-assets developed by international standard-setting bodies or in the EU[48]. Several standard setters adhere to a distinction along the following three categories:

- Exchange token: formerly often referred to as VCs or crypto-currencies. Typically, they do not provide rights (as is the case for investment or utility tokens) but are used as a means of exchange (e.g. to enable the buying or selling of a good provided by someone other than the issuer of the token) or for investment purposes or storage of value.
- Security token: typically do provide rights (e.g. in the form of ownership rights or entitlements similar to dividends). For example, for capital raising, asset tokens may be issued in the context of an ICO which allows businesses to raise capital for their projects by issuing digital tokens in exchange for fiat money or other crypto-assets.
- Utility token: typically enable access to a specific product or service, often provided using a DLT platform, but not accepted as a means of payment for other products or services.

This distinction is, however, schematic and hence imprecise. Some assets have features spanning more than one of these categories, or that change during the lifecycle of the asset.[49] Also, assets with new features may evolve over time, for example the pegging of crypto-assets

---

[46] EBA, *Opinion on 'virtual currencies'*, EBA/Op/2014/08, 4 July 2014 stating that the term 'virtual currency' shall be regarded as "*a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a FC [fiat currency], but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically*"; Bank for International Settlements, *Digital currencies (2015)* < *https://www.bis.org/cpmi/publ/d137.pdf*> | *Accessed 4 November 2019*; Banque de France, *The dangers linked to the emergence of virtual currencies: the example of bitcoins (2013)* < https://www.banque-france.fr/sites/default/files/medias/documents/focus-10_2013-12-05_en.pdf> | Accessed November 2014; Banque de France, *The emergence of bitcoin and other crypto-assets: challenges, risks and outlook (2018)* <*https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_en.pdf*> | Accessed 4 November 2019; Mark Carney, *Speech: The Future of Money* (2018) <https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-future-of-money-speech-by-mark-carney.pdf?la=en&hash=A51E1C8E90BDD3D071A8D6B4F8C1566E7AC91418> | Accessed 5 November 2019; Rainer Böhme and others, *Bitcoin: economics, technology, and governance*, Journal of Economic Perspectives [2015], Vol. 29(2), 213-38; Malcolm Campbell-Verduyn, *Bitcoin and Beyond*, Routledge, 2018.

[47] Financial Stability Board, *Crypto-asset markets: Potential Channels for future financial stability implications* (2018) < https://www.fsb.org/wp-content/uploads/P101018.pdf> | Accessed 6 November 2019

[48] Financial Stability Board, *Crypto-assets: Work underway, regulatory approaches and potential gaps* (2019) <https://www.fsb.org/wp-content/uploads/P310519.pdf> Accessed 5 November 2019; Financial Stability Board, *Crypto-assets regulators directors (2019)* < *https://www.fsb.org/wp-content/uploads/P050419.pdf*> | Accessed 5 November 2019; Financial Stability Board, *Crypto-assets: Report to the G20 on the work of the FSB and standard-setting bodies (2018)* < https://www.fsb.org/wp-content/uploads/P160718-1.pdf > | Accessed 3 November 2019

[49] European Banking Authority, *Report with advice for the European Commission on crypto-assets* (2019) < https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1> | Accessed 6 November 2019;

to a basket of 'real' assets such as currencies. More fundamentally, this distinction has been developed mainly with a view to comparing the regulatory treatment of crypto-assets to the treatment of existing asset categories: 'exchange tokens' may be regulated like payment/money; 'security tokens' may be regulated like financial instruments; 'utility tokens' are typically unregulated. However, also this comparison of categories is not perfect and regulators agree that the assessment of crypto-assets needs to be made on a case-by-case basis.[50] As our Group takes a functional view of risks and opportunities arising from technology-enabled financial services, this report does not make use of the three categories in the further analysis.

Crypto-assets, though different in detail, are built on similar technological concepts, regardless of whether they represent an entitlement against someone or a 'virtual' value:[51] (a) they are individually identifiable, (b) some, especially more recent ones, can carry complex information in respect of the entitlement, including auto-executable functions regarding governance and payment, such as interest payment,[52] (c) they are typically, but not necessarily, stored in distributed financial networks using DLT/Blockchain technology, (d) holdings and transactions history are protected by means of cryptography.

The perception of the advantages with the use of crypto-assets depends significantly on the concrete case, and promoters of crypto-asset-based solutions follow different rationales:[53]

a. For most market participants developing crypto-assets, cost saving is the most important argument. Notably, they provide for a common workflow that allows participants more direct access to assets leading to efficiency gains, faster processing of instructions (e.g. re transfers), and more direct access. Intermediary functions can be abolished, and there is little or no need for so-called 'back-offices' sorting out the details of asset holding and dispositions, including processing of corporate rights, or reconciliation in case of mismatch.[54] Generically, the technology in effect enables a simulated vertical integration and common workflow;

b. Security of holdings is a second important argument. Records can be designed to be tamper-resistant, and the distributed nature of the record avoids the problem of a single point of failure;

c. Lastly, crypto-assets are used as a means of capital raising, in the form of so-called 'ICOs'. This type of investment seems highly attractive and credible to some parts of the internet-savvy generations, motivating issuers to use crypto-assets instead of

[50] EBA, ibid.

[51] Financial Stability Board, *Crypto-asset markets: Potential Channels for future financial stability implications* (2018) < https://www.fsb.org/wp-content/uploads/P101018.pdf> | Accessed 6 November 2019

[52] In particular, assets created on the 'Ethereum network'.

[53] For others, notably so-called virtual currencies such as Bitcoin, the remoteness from regulators and law enforcement, central banks and the regulated private financial sector is an important part of the rationale to create them. In this respect, see Nigel Dodd, *The Social Life of Bitcoin [2018]* Theory, Culture & Society, Vol.35(3), 35-56.

[54] Phillip Paech, *The Governance of Blockchain Financial Networks [2017]* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875487.

traditional financing sources, which may allow to avoid closer scrutiny of their business models.[55]

The regulated financial sector, such as banks, insurance companies and other types of financial institution, contemplate the use of crypto-assets for the first and second reason. For instance, banks have been piloting DLT-based solutions, including a crypto-asset components in the context of trade finance, coordination of payments across internal balance sheets, syndicated loans, green bond issuance and consumer-facing offerings. Some market infrastructure providers have also been testing DLT for the issuance, admission and trading of equity securities, and evidencing the change of beneficial ownership settlement, corporate actions like proxy voting and shareholder transparency.[56]

Firms coming from beyond the traditional financial sector, and which are typically unregulated or lightly regulated, have also been entering the market to offer services relating to crypto-assets such as ICOs, custodian wallet services and trading platforms.[57] They often operate outside the perimeter of financial regulation, such as disclosure and consumer protection rules, client asset protection or rules on adequate governance arrangements and operational soundness. As a consequence, risks for investors or customers are typically higher than for regulated financial products and services. Where these risks have materialised in the past, relevant investors or users have suffered losses.[58]

EBA and ESMA observed risks to the level playing field as Member States start to introduce their own national legislation in this field. Divergences at the national level, including taking account of developments in third countries, create uncertainty for consumers and firms, and also scope for regulatory arbitrage (c.f. Recommendations on fragmentation).[59] The ESAs also

---

[55] Nare Essaghoolian, *Initial Coin Offerings: Emerging Technology's Fundraising Innovation [2019]* UCLA Law Review, Vol. 66(1), 294-344; Consob, Call for evidence: '*Initial Coin Offerings and Crypto-Assets Exchanges*' [2019] < http://www.consob.it/documents/46180/46181/doc_disc_20190319_en.pdf/e981f8a9-e370-4456-8f67-111e460610f0 > | Accessed 5 November 2019; BaFin, *Initial Coin Offerings: Advisory letter on the classification of tokens as financial instruments (2018)* <https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs_en.pdf?__blob=publicationFile&v=2>; Accessed 5 November 2016

[56] Federico Panisi and others, *Blockchain and Public Companies: A Revolution in Share Ownership Transparency, Proxy-Voting and Corporate Governance?* [2019] Stanford Journal of Blockchain Law & Policy < https://stanford-jblp.pubpub.org/pub/blockchain-and-public-companies> | Accessed 5 November 2019;

[57] European Securities and Markets Authority, *Advice: Initial Coin Offerings and Crypto-Assets (2019)* < https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> Accessed 5 November 2019; Financial Stability Board, *Crypto-assets: Report to the G20 on the work of the FSB and standard-setting bodies (2018),* 5-6, < https://www.fsb.org/wp-content/uploads/P160718-1.pdf> |Accessed 5 November 2019

[58] OECD, *Initial Coin Offerings (ICOs) for SME Financing* (2019) < www.oecd.org/finance/ICOs-for-SME-Financing.pdf> | Accessed 5 November 2019.

[59] Jurisdictions are starting to establish regulatory frameworks for specified types of crypto-asset business. For example the French Plan d'Action pour la Croissance et la Transformation des Entreprises (PACTE – Action Plan for Business Growth and Transformation) is intended to facilitate access to diversified funding, including by establishing an optional visa regime for ICOs and optional license scheme for digital asset service providers (see https://www.amf-france.org/en_US/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France?langSwitch=true). In Malta, the Virtual Financial Assets Act establishes three types of authorisation requirement: (i) registration of VFA Agents, (ii) registration of Whitepapers, and (iii) registration of VFA Services Providers with the objective of supporting the innovation and new technologies for financial services in the area of crypto-assets whilst ensuring effective investor protection, financial market integrity and financial stability: https://www.mfsa.mt/fintech/virtual-financial-assets/. Liechtenstein's Law on Tokens and TT Service Providers (TVGT: Das Token- und VT-Dienstleistungsgesetz) is intended to "ensure trust in digital legal communication, in particular in the financial and economic sector, and the protection of users of TT [trustworthy technologies] systems" and to "create an optimal, innovation-friendly, and technology-neutral framework for rendering services on TT [s]ystems." For that purpose, it addresses civil law questions regarding tokens, the representation of rights via tokens, and the transfer of tokens and establishes a framework for the supervision of TT service

identified a loss of opportunity from the absence of an EU regime, noting challenges to the scaling-up of cross-border activities in the absence of a common approach with regard to factors such as accounting treatment, conduct of business, including client asset rules, prudential treatment,[60] custody and transaction finality, insolvency treatment, and tax.

In particular, the treatment of crypto-assets or tokenised settlement arrangements is important for the applicability of the financial market acquis, spanning from bank capital requirements to trading venue regulation, finality, collateral and consumer protection rules.

So far, regulators and legislators have struggled to classify crypto-assets within existing laws and regulatory schemes[61], and even where national rule makers attempt to progress on that question, such attempts can only provide isolated solutions in a highly internationalised market.

For example, if a crypto-asset qualifies as a financial instrument under MiFID, the execution of orders is subject to MiFID and the entity providing order execution services has to be licensed as an investment firm. In addition, transactions in crypto-assets which qualify as transferable securities and are admitted to trading/traded on a trading venue have to be registered in the book-entry system of a duly licensed central securities depository. In order to know whether a crypto exchange qualifies as a MiFID trading venue (regulated market, MTF or OTF), the processes and procedures of such exchanges need to be reviewed in light of existing legal definitions.

However, in order to determine the legal qualification of a crypto-asset or an exchange, a substance-over-form approach needs to be taken: a product/service with the same or similar characteristics as an existing one needs to be treated in the same way from a regulatory perspective. Likewise, if a crypto-asset qualifies as a transferable security, a public offering thereof is subject to the Prospectus Regulation and a prospectus needs to be published and pre-approved by the competent authority.

To avoid fragmentation of the European market, a common taxonomy and approach on the application of existing EU acquis (and, where appropriate, extension of the EU perimeter) is urgently needed to ensure a more consistent and comprehensive regulatory treatment.

*Ensure appropriate regulation of activity involving crypto-assets*

In the EU, the EBA and ESMA published in January 2019 reports setting out their assessments of the applicability and suitability of EU law to crypto-assets, reporting on issues relating to banking, payments, e-money, AML/CFT requirements and ICOs and securities and markets

---

providers: https://www.llv.li/inhalt/118563/amtsstellen/schaffung-eines-gesetzes-uber-token-und-vt-dienstleister-token-und-vt-dienstleister-gesetz-tvtg-und-die-abanderung-weiterer-gesetze-bua-0542019. See also UK Judicial Taskforce, legal status of crypto-assets and smart contracts https://www.judiciary.uk/announcements/the-chancellor-of-the-high-court-sir-geoffrey-vos-launches-legal-statement-on-the-status-of-cryptoassets-and-smart-contracts/

[60] https://www.bis.org/bcbs/publ/d490.htm

[61] Financial Stability Board, *Crypto-asset markets: Potential Channels for future financial stability implications* (2018) < https://www.fsb.org/wp-content/uploads/P101018.pdf> | Accessed 6 November 2019; The Library of Congress, Regulation of Cryptocurrency Around the World (2018) < https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf> | Accessed 6 November 2019; The Law Library of Congress, *Regulation of Cryptocurrency Around the World*, (2018) < https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf> | Accessed 5 November 2019.

laws, including MIFID.[62] These build on earlier reports and advice of the ESAs and previous warnings to consumers and financial institutions about risks arising from activities involving crypto-assets.[63] The EBA and ESMA conclude that some crypto-assets may qualify as financial instruments under MiFID or as electronic money under EMD2, or may fall outside the scope of EU financial services law. But even where crypto-assets fall outside the scope of current EU financial services law, AML/CFT legislation (AMLD5[64]) may still apply.

Our Group agrees with EBA and ESMA and recommends that the Commission take action to assess whether changes to EU law are needed to address uncovered risks, or to clarify the application of existing rules, including:

- AML vulnerabilities;[65]
- Pegging and conversion: Crypto-assets backed by traditional financial assets (currency or securities), which may be deemed so-called 'stablecoins', may pose systemic risks in the form of currency risk. Depending on the nature of the pegging arrangements, such assets, in particular if adopted at scale, may pose a risk to financial and monetary policy. Further, it may be unclear how, for example, foreign exchange rules and regulations will apply. The user needs to have the ability to redeem the crypto-asset into the underlying fiat currencies or other assets it is pegged to; however, jurisdictions will have different currency constraints and also varying foreign exchange management. In addition, each stablecoin will affect the foreign exchange reserves of the respective holders' countries. Less developed nations do not dispose of foreign exchange reserves and they often limit or curb the acquisition of a foreign currency. Therefore, in such jurisdictions, it is unclear how convertibility will function and which downstream financial system implications this would introduce;
- Regulated financial institutions' exposures to crypto-assets[66]**:** currently there is no clarity as to the appropriate prudential treatment of financial institutions' exposures to crypto-assets that are not subject to EU law. This lack of clarity poses a barrier to institutions', who may be considering gaining exposures in the context of different

---

[62] European Banking Authority, *Report with advice for the European Commission on crypto-assets* (2019) https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1 | Accessed 6 November 2019; European Securities and Markets Authority, *Advice: Initial Coin Offerings and Crypto-Assets* (2019) < https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> | Accessed 6 November 2019.

[63] European Banking Authority, *Warning: ESMA, EBA & EIOPA warn consumers on the risks of virtual currencies* (2018) < https://eba.europa.eu/sites/default/documents/files/documents/10180/2139750/313b7318-2fec-4d5e-9628-3fb007fe8a2a/Joint%20ESAs%20Warning%20on%20Virtual%20Currencies.pdf?retry=1> | Accessed 6 November 2019.

[64]Directive (EU) 2018/843 of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (2018) OJ L 156,43–74.

[65] Financial Action Task Force, Public Statement – Mitigating Risks from Virtual Assets http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html |; European Banking Authority, *Report with advice for the European Commission on crypto-assets* (2019) < https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1> | Accessed 6 November 2019;

[66] Bank for International Settlements, *Statement on Crypto-Assets* (2019) < https://www.bis.org/publ/bcbs_nl21.htm> | Accessed 6 November 2019

business activities and should be addressed at the EU level in order to ensure a common approach.

- Consumer protection: currently consumers typically lack adequate protection when engaging with crypto-asset products and services falling outside the existing EU regulatory framework. For example, often they do not receive clear disclosures of risk involved in a specific crypto-asset or their rights and protections (if any) e.g. in the event of the insolvency of an issuer. Inevitably the absence of consistent protections limits the interests of consumers in crypto-asset products and services and results in an un-level playing field as national measures emerge to protect local consumers, further limiting the capacity for the scaling of products and services across the Single Market.

From our Group's perspective, the most important factor of the EU's approach to crypto-assets is a uniform one, based on the principle that activities that create the same risks should be governed by the same rules, thus avoiding fragmentation in this regard. This is necessary to avoid associated risks, including regulatory arbitrage, comprehensively, and to avoid a race to the bottom in terms of stringency of regulation. Further, only a uniform approach to regulating crypto-assets will be able to unlock the benefits of innovation, allowing market participants to benefit from scaling effects. At the same time, the EU must co-ordinate with its international partners in this regard, bearing in mind the inherently borderless nature of the technologies and need for international consistency, necessary for technology-based solutions entailing crypto-assets to be rolled out across international groups or in the context of, for example, international supply chains or in the trade finance context. This includes, most importantly, the conflict-of-laws question.

***Recommendation 8 – Commercial law of crypto-assets***

***In order to ensure market participants' rights and to guarantee a meaningful application of the commercial law concepts established in EU regulation (such as InsR, SFD, FCD, BWUD, BRRD) to crypto-assets which are held on a distributed financial network, the Commission, in co-operation with the ESAs and international standard-setting bodies and other relevant authorities, should:***

***a. legislate a relevant conflict-of-laws rule, ideally enshrined in a Regulation, and,***

***b. consider which further aspects of the commercial law regarding such networks and regarding the assets administered on them should be addressed at EU level.***

*Background*

DLT/Blockchain networks are not a law-less space, as is sometimes claimed, in particular where commentators regard these networks from the purely technical or ideological angle. Recent failures of some intermediaries acting in the sphere of crypto-assets have shown that in the event of insolvency, in particular, the same issues arise as to 'who owns what' as typically arise in relation to securities, cash or other financial assets.

The commercial law framework, including property, corporate and insolvency law, does apply to these situations. However, the novelty of the distributed concept renders the application of these areas of law uncertain and unpredictable. This is, first, because of the international nature of the relevant issues. The second reason is that the disappearance of the established two-party relationship as a kernel of each financial arrangement: the general law is entirely built on this bilateral understanding of relationships. In that sense, the situation is comparable to the issues described in the context of Recommendation 6.

Commercial law is to a large extent the Member States' national autonomous law. A fully-fledged EU-wide legal framework is difficult to establish and probably neither necessary nor desirable. However, a number of questions need a common legal answer.

This applies, first and foremost, to the question of which (national) law applies to a given real-world situation, for example the proprietary situation of client assets held on a distributed network. These so-called conflict-of-laws rules make sure that in international situations, courts know which law to apply. It is crucial for parties to know from the outset, *ex ante*, with certainty, which law that will be, in order to be able to draft legal documentation accordingly. To this end, a clear criterion determining the law applicable to assets held on distributed networks must be defined. In order to provide the highest degree of predictability and in order to avoid situations in which different courts come to different views, this criterion should ideally be uniform (as opposed to only 'similar') throughout all jurisdictions of the EU. Solutions include criteria such as the regulatory jurisdiction of the operator of the network, the issuer's jurisdiction or a limited choice of law made by the participants of the network.

Beyond that, the Commission and ESAs should assess whether a meaningful application of the remainder of commercial law, including property, corporate and insolvency law aspects, requires further targeted harmonisation. One important aspect relates to ownership of assets held on a distributed financial network, in particular crypto-assets. While the technology may suggest direct ownership of a particular crypto-asset, a clear legal structure must still exist to confer rights onto the token holder, extending to the underlying real-world assets (if any) held through custodial structures.

The clarification of commercial law relationships, including the conflict of laws question, is relevant beyond the issue of individual market participants' legal position. It has a wider regulatory, and even systemic importance. Risk management of financial institutions is built on the understanding that rights are enforceable in court. Core EU financial regulation, such as CRD, FCD, SFD is firmly built on this fundamental understanding. Other EU rules, in particular the BRRD, are heavily dependent on a proper functioning of commercial and corporate law[67].

It is therefore important that the application of commercial law to crypto-assets be clarified. In order to facilitate the creation of an internal market for crypto-assets held on distributed financial networks, thereby enabling holdings of crypto-assets across the EU, a common approach to these issues is indispensable.

---

[67] Philipp Paech, *The International Law of Crypto-Asset Settlement*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2792639

## *Standardisation, RegTech and SupTech*

### ***Recommendation 9 – RegTech and SupTech***

***The Commission, in cooperation with the ESAs, and in co-ordination with relevant authorities and international standard setters, should develop and implement a comprehensive and ambitious agenda to support the adoption of advanced RegTech and SupTech by the financial sector.***

*Background*

Financial institutions face ever-increasing and tighter regulatory constraints on their activities from regulators and supervisors globally. There is an increasing recognition that digital technologies offer significant cost savings for firms to perform what are currently labour intensive, manual regulatory compliance and reporting processes.[68] Digital technologies also offer regulators and supervisors opportunities to automate and make more efficient and effective regulatory and supervisory processes.[69] The terms RegTech and SupTech refer to the new categories of digital technologies that make regulatory compliance and reporting, on the one hand, and supervisory processes and risk analysis, on the other, more efficient and cost effective.[70] Digital regulatory compliance and digital regulatory reporting are now possible, with core technologies such as AI and DLT, in conjunction with enabling technologies such as cloud.

The terms 'RegTech' and 'SupTech' refer to technology-enabled regulatory and supervisory processes (they are used here without delimiting one from the other) that have the potential to create efficiencies in compliance, regulatory reporting and risk analysis[71]. Since the financial

---

[68] Tom Butler & Leona O'Brien, *Understanding RegTech for Digital Regulatory Compliance* [2019] Disrupting Finance, 85-102; Douglas W. Arner and others, *FinTech, RegTech and the reconceptualization of financial regulation* [2017] Northwestern Journal International Law & Business, Vol. 37(3), 371-413.

[69] Dirk Broeders & Jermy Prenio, *Innovative technology in financial supervision (SupTech) — The experience of early users* (2018) < https://www.bis.org/fsi/publ/insights9.pdf> | Accessed 20 June 2019

[70] European Securities and Markets Authority, *Report: Trends, Risks and Vulnerabilities* (2019) < https://www.esma.europa.eu/sites/default/files/library/esma50-report_on_trends_risks_and_vulnerabilities_no1_2019.pdf > | Accessed 20 June 2019; Douglas W. Arner and others, *FinTech, RegTech and the reconceptualization of financial regulation* [2017] Northwestern Journal International Law & Business, Vol. 37(3); Financial Conduct Authority, *Regulatory sandbox lessons learned report* (2017) < https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf> Accessed 21 June 2019; BaFin, *Big data meets artificial intelligence: Challenges and implications for the supervision and regulation of financial services* (2018) < https://www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.pdf;jsessionid=C6108799C8B0C3E50F5A57BB542BD792.2_cid290?__blob=publicationFile&v=11> | Accessed 21 June 2019; Susan Athey, *Beyond prediction: Using big data for policy problems* [2017] Science, Vol. 355, Issue 6324

[71] European Securities and Markets Authority, *Report: Trends, Risks and Vulnerabilities* (2019) < https://www.esma.europa.eu/sites/default/files/library/esma50-report_on_trends_risks_and_vulnerabilities_no1_2019.pdf > | Accessed 20 June 2019; Douglas W. Arner and others, *FinTech, RegTech and the reconceptualization of financial regulation* [2017] Northwestern Journal International Law & Business, Vol. 37(3); Financial Conduct Authority, *Regulatory sandbox lessons learned report* (2017) < https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf> Accessed 21 June 2019; BaFin, *Big data meets artificial intelligence: Challenges and implications for the supervision and regulation of financial services* (2018) < https://www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.pdf;jsessionid=C6108799C8B0C3E50F5A57BB542BD792.2_cid290?__blob=publicationFile&v=11> | Accessed 21 June 2019

crisis, compliance requirements for regulated financial service providers have been strengthened. Between 2008-2016, there was a 500 percent increase in regulatory changes in developed markets, highlighting the need for scalable, reliable and efficient RegTech solutions. As firms seek to reduce compliance burdens and avoid regulatory fines research, by Juniper Research, found that over the next few years RegTech spend will grow by 48 percent per annum – rising from $10.6 billion in 2017 to $76.3 billion in 2022.[72] For example, reporting requirements have been significantly increased in order to address the data gaps that left firms and supervisors unable to spot at an early stage the build-up of risks in the financial system.[73]

Albeit essential, the current framework is inefficient. Reporting requirements:

- have to be translated into firms' systems and controls using manual procedures which can be both error-prone (input errors, subjective interpretations applied to data terms) and time consuming;
- may be duplicative, requiring firms to report in different contexts (and potentially using different templates and time series) the same data to different supervisors (including beyond the financial sector);
- may result in the transmission to supervisors of data that is erroneously or inconsistently reported (as a result of the above), causing delays to data processing and analysis and prompting extensive data cleaning (often manual) or re-submission.

Technology-enabled innovation can help overcome these challenges[74] by enhancing efficiencies in reporting and compliance through:

- machine readable and machine executable legislation (see further below) involving the standardisation of regulatory instructions in a machine executable version which can facilitate automated regulatory reporting by firms[75] [76];

---

[72] Nicole Sandler, *RegTech Collaboration: Making the future of innovative compliance a reality*, CIO Applications Europe <https://ibm.cioapplicationseurope.com/cxoinsights/regtech-collaboration-making-the-future-of-innovative-compliance-a-reality-nid-1537.html> | Accessed 19 June 2019

[73] Andrea Sironi, *The Evolution of Banking Regulation Since the Financial Crisis: A Critical Assessment* [2018] BAFFI CAREFIN Centre Research Paper No. 2018-103; Bank for International Settlements, *CGFS Papers No. 60 - Structural changes in banking after the crisis* (2018) < https://www.bis.org/publ/cgfs60.pdf> |Accessed 22 June 2019; Gerard Caprio, *Financial regulation after the crisis: how did we get here, and how do we get out?* [2013] Federal Reserve Bank of San Francisco, Issue Nov, pp. 1-49.

[74] Financial Conduct Authority, *Digital regulatory reporting* (2017) < https://www.fca.org.uk/digital-regulatory-reporting> |Accessed 22 June 2019

[75] Financial Conduct Authority and others, *RegTech Sprint Technology Roundtable*: *Model Driven Machine Readable and Executable Regulatory Reporting* (2018) < https://www.gr3c.com/wp-content/uploads/2018/04/RegTech-Sprint-Technology-Roundtable-Dublin-April-5th-Proceedings.pdf> | Accessed 22 June 2019

[76] For instance, in 2018 the UK the FCA issued a call for inputs to assess the current compliance burden for regulatory reporting with the aim of reshaping it in a more efficient manner.

Financial Conduct Authority, *Call for Input: Using technology to achieve smarter regulatory reporting* (2018) < https://www.fca.org.uk/publication/call-for-input/call-for-input-smarter-regulatory-reporting.pdf > | Accessed 23 June 2019; Financial Conduct Authority, Financial Conduct Authority, *Digital Regulatory Reporting: Feedback Statement on Call for Input* (2018) < https://www.fca.org.uk/publication/feedback/fs18-02.pdf> | Accessed 23 June 2019; Financial Conduct Authority, *Digital Regulatory Reporting Pilot: Terms of Reference* (2018) < https://www.fca.org.uk/publication/minutes/digital-regulatory-reporting-pilot-terms-of-reference.pdf> | Accessed 23 June 2019;

- automated and AI solutions for data input, aggregation and analysis, including solutions enabling 'straight through processing' of regulatory returns[77];
- platforms which link regulation, compliance processes and reporting (regulatory clearing house, see below).

The benefits of such solutions include:

- greater accuracy and efficiency in reporting and data analysis and, in turn, more timely risk analysis and mitigation;
- faster and lower-cost regulatory reporting (for firms, potentially also lowering barriers to entry and potentially enhancing competition) and data processing (for firms and supervisors);
- more effective regulation and supervision (time factor, quality factor) for all regulatory areas, in particular prudential, consumer protection, market integrity, AML and CFT, etc.

The adoption of standards-based common RegTech and SupTech solutions would assist firms (e.g. in day-to-day regulatory reporting), supervisors (e.g. in analysing suspicious transaction reports, reported data and data-sharing cross-border), and the ESAs (e.g. in the context of the reporting of data for stress test exercises and the monitoring of macro prudential risks).

Currently, the regulatory framework in the EU does not directly address the RegTech or SupTech paradigms,[78] and the approach taken by firms and supervisors to pilot and adopt RegTech and SupTech frameworks is currently ad-hoc and uncoordinated. These inconsistencies pose a barrier to the realisation of full efficiency gains of RegTech and SupTech solutions. For instance, a financial conglomerate with subsidiaries in more than one jurisdiction is currently unlikely to be able to roll out the same reporting solution for all businesses in the group, due to different supervisory expectations and technological capacities.

Therefore, the Group recommends that the EU develops and implements a comprehensive and ambitious agenda for the establishment of advanced RegTech and SupTech capabilities, in co-ordination with relevant authorities in and beyond the EU and international standard setters.

[77] A key part of risk management functions is the modelling, definition and analysis of scenarios and forecasting exercises. This can also serve as a supervisor's use case. Another use case for supervisors is the use of AI technology for natural language processing, which allows for easier analysis of banks' or other institutions' reports to identify information relevant for supervision.

[78] European Securities and Markets Authority, *Developments in RegTech and SupTech* (2018) < https://www.esma.europa.eu/sites/default/files/library/esma71-99-1070_speech_on_regtech.pdf> | Accessed 23 June 2019; Bank of International Settlements, *Fin-RegTech: Regulatory challenges with emphasis on Europe* (2019) < https://www.bis.org/review/r190318m.pdf > | Accessed 22 June 2019; Bank of International Settlements, *Financial inclusion and the FinTech revolution: implications for supervision and oversight* (2016) < https://www.bis.org/speeches/sp161026.pdf> | Accessed 22 June 2019

***Recommendation 10 – Standardisation of legal terminology and classification of actors, services, products and processes***

***The Commission, in co-operation with the ESAs and the ESCB, should facilitate initiatives that promote standardisation of legal terminology and digital standards-based common classifications of actors, services, products and processes in the financial sector for use by market participants, regulators, supervisors and standard setters.***

*Background*

In order to support a truly integrated digital technology-enabled Single Market for financial services, a common language is required to facilitate digital communication among financial institutions and other market participants, regulators and supervisors. This is a *conditio sine qua non* for interoperability between digital services and products, and to make regulation and supervision more efficient and effective. However, currently FinTech, RegTech and SupTech are not underpinned by a common language and a common rulebook. The industry has, created a *Tower of Babel (Haldane)*,[79] which refers to the absence of a 'common language' in the financial industry, and the existence of heterogeneous terms and concepts to describe similar business objects, processes and products. This problem permeates the industry down to individual financial institutions, where products, concepts and terms have different meanings in and across business functions and communities of practice. The emergence of FinTech, RegTech and SupTech will do little to solve fundamental problems if the industry ends up with that digital *Tower of Babel*, simply digitising the status quo. These gaps and inconsistencies between the multiple heterogeneous languages in use across the financial industry and the regulatory/supervisory sphere represent a major inhibitor to the scaling up of FinTech innovation across the EU, while also presenting a barrier for new entrants. There are currently several initiatives aiming to promote greater standardisation[80] – however, their precise reach and ambition remain so far unclear.

For these reasons the Group recommends that the Commission should facilitate initiatives that promote the development of digital standards-based common classifications of actors (including duties and responsibilities), services, products, and processes in the financial sector for use by financial service providers, FinTechs, regulators, supervisors and standard setters. In taking forward this work, the Commission should draw inspiration from the aviation, telecommunications and pharma sectors which provide compelling examples of how regulators and industry can lower industry costs and increase interoperability and innovation through standards co-created with regulators.

[79] Bank of International Settlements, *Towards a common financial language* (2012) < https://www.bis.org/review/r120315g.pdf> | Accessed 24 June 2019

[80] In the financial sector, some standard setters have commenced work on relevant proposals, e.g. BIRD (ESCB), FIRDS (ESMA), and Financial Data Standardisation (DG FISMA).

***The role of Digital Taxonomies, Vocabularies and Ontologies in capturing knowledge of business, legal and regulatory concepts.***

*Innovation in aviation, telecommunications, life sciences and pharmaceutical sectors is enabled by the existence of common, generally accepted definitions of the core concepts employed in related disciplines. The application of existing and emerging digital technologies such as AI, Smart Contracts, IoT and Quantum Computing is enabled significantly by the existence of common language, for example in the field of medicine. Even the ubiquitous Internet would not have developed in the manner it has without the generally agreed, standards-based approaches to innovation and a common technical language. The World Wide Web Consortium (W3C) standards were pivotal. The same standards can be applied to develop common taxonomies, vocabularies and ontologies that can capture knowledge about the financial industry in digital format that is both human readable and machine-computable.*

*There are no generally accepted classifications or taxonomies of actors, activities, processes and products or services in the financial industry. Existing, standards-based semantic technologies can help harmonise and provide an integrative platform for taxonomies, vocabularies and ontologies that act as an overarching structure for FinTech-enabled business and financial regulation and supervision.*

***Recommendation 11 – Human- and machine-readable legal and regulatory language***

***The Commission, in co-operation with the ESAs, should adopt a strategy on how reporting and compliance processes may become both machine- and human-readable, to the extent possible.***

*Background*

Historically the legislative framework has been developed on the basis of human-, rather than machine-, readable text. This limits the potential for the development of automated compliance and reporting tools (e.g. due to imprecision in the language used and coding difficulties) and creates inefficiencies as data outputs often need to be translated into human language to ultimately check compliance.

To support greater accuracy and efficiency in compliance and reporting processes, action is needed to progress the development of legislation that is both human- and machine-readable.

Legal, regulatory and business vocabularies will need to be harmonised and digitised using common technical standards, if they are to be machine-readable and, where necessary, machine-computable. This will require collaboration between EU authorities and national competent authorities working with financial institutions to develop a common financial dictionary/language and reporting requirements, on the basis of common taxonomies, vocabularies and ontologies. The objective of instituting Digital Regulatory Reporting currently

being pursued by UK regulators is based on the premise of regulations being not only human-readable and machine-readable, but also machine-computable.[81] This novel approach would allow much of the supervisory, regulatory, and capital reporting to be automated, enabling the straight-through processing of regulatory reporting.

This will require collaboration between EU authorities and national competent authorities working with financial institutions to develop a common financial dictionary/language and reporting requirements, on the basis of a common taxonomy and ontology (see above).

The Group recognises that conception and implementation of this recommendation is a long-term project and transitional arrangements will be needed in view of the significant upfront costs for firms and supervisors when adjusting to new compliance and reporting frameworks.

As the enablers of RegTech and SupTech, standardisation, machine-readable common language and interoperability are interlinked, a holistic and top-down review is needed to investigate the feasibility of enhancing reporting and data analysis using these solutions.

***Recommendation 12 – Regulatory Clearing House***

***The Commission, in co-operation with the ESAs and the ESCB, should adopt a strategy for the conception and establishment of regulatory clearing houses, i.e. arrangements capable of***

- ***centralising the automated dissemination of rules to regulated entities,***
- ***receiving incident and reporting information from regulated entities, and***
- ***collecting market data.***

*Background*

Following the financial crisis, firms faced voluminous and heterogeneous sets of regulations, on one hand, and reporting requirements for significantly expanded data sets on transactions and macro-and micro-prudential risks, on the other. Regulators and supervisors also face complexity in producing regulations and in processing ever growing and complex data pools. To complicate matters, firms submit the same data to multiple supervisors for different purposes, or may make the data available to one supervisor, but it is relevant to the work of others and cannot be readily accessed or, where it can be accessed, may result in duplicative data analysis.

To support greater efficiencies in data access, aggregation and analysis, the Group recognises, as another longer-term initiative, the benefits of exploratory work on the establishment of an EU regulatory clearing house. Such an arrangement could centralise and streamline both the dissemination of reporting (and other regulatory) requirements and the submission and analysis of reporting data.

[81] Tom Butler, & Leona O'Brien, *Understanding RegTech for Digital Regulatory Compliance* [2019] Disrupting Finance, 85-102

Beyond the centralisation and streamlined capture and dissemination of reporting data, regulatory clearing houses could also be used to disseminate regulatory rules amongst market participants. Rules are currently made available through conventional (e.g. paper or web-based) channels, and in human readable language. A regulatory clearing house could not only push human readable rules to regulatees in real time, but also, ideally, in machine-readable and computable rules in a common language.

In future, the potential of FinTech, RegTech and SupTech may be extended to not only making rules available via digital channels, but also to see them implemented by digital processes directly, while at the same time compliance and reporting data is provided back to the supervisors via digital channels. Thus, the "consumption" of rules, including technical standards and guidelines and the submission of regulatory compliance data, could be entirely automated for standard cases.

# Maintaining a Level Playing Field

Technology-driven change may provoke a need to adapt financial regulation, in order to ensure a level playing field between incumbents and new market entrants and between different types of market participants, including the need to ensure that consumers using interchangeable products receive comparable protection. Incumbent institutions have always embraced IT innovation to such an extent that the more financial institutions digitize their front, middle and back offices, the more they become like technology or software companies. At the same time, innumerous new entrants become active on the financial market, enabled by innovative technologies, which in some cases are subsidiaries of incumbent well-established financial institutions, whereas in other cases new entrants are start-ups, entirely independent from existing financial institutions. At the other end of the scale, large technology companies, particularly BigTechs such as Google, Amazon, Facebook and Apple, are lining up to enter the financial industry directly or in some cases in partnership with financial institutions. They compete on what could be described as traditional financial products and services, while at the same time innovative products and services may emerge that have features that resemble regulated products and services. The latter may fall outside the scope of current EU law, as their technology-enabled characteristics may take them outside the boundaries of the relevant requirements.

In short, the market provides products and services subject to differing regulatory frameworks and the rules applying to market participants may diverge substantially – even where the products and services are functionally similar from a user perspective. This situation is currently materialising, and EU regulation must hence ensure a level playing field.

## *Regulatory approach*

### ***Recommendation 13: Activity and risk-based regulation***

***The Commission and the ESAs should take the necessary steps to ensure that regulation of the financial sector follows the principle of 'same activity creating the same risks should be regulated by the same rules'.***

*Background*

Different types of financial service provider compete, notably incumbents and new market entrants, including BigTechs such as social networks or online market places, and small or new entrants, concentrating on tech-enabled financial services. They may be subject to markedly different standards, notably because they may be authorised in different Member States under different, entities-based EU regimes (credit institutions, payment institutions (see box on p17),

e-money providers, etc.), or because the relevant activity may be outside the EU regulatory perimeter, subjecting them to autonomous national regulation (if any).

***Example: Prudential framework***

*The prudential regulatory framework requires compliance by groups of credit institutions on a consolidated basis (Art. 18 CRR). Credit institutions, financial institutions and ancillary services undertakings that belong to a banking group have to apply banking-level controls, no matter what their activity or the actual risks involved. This differs from the regulatory scheme in some jurisdictions, such as the US, where bank and financial services holding companies have a different regulatory perimeter from the bank itself and, as a result, certain parts of the business of the group are not necessarily consolidated e.g. for the purposes of capital requirements.*

*Non-bank financial service providers performing the same activities entailing the same risk would be subject to activity-based regulation, but not to the prudential framework. This may lead to results such as banks' subsidiaries facing difficulties in attracting and retaining talent, or might incur higher costs and time-to-market to deliver innovation as a result of bank-grade pay restrictions even for non-risk related functions, requirements for internal control, risk management or outsourcing requirements. Additionally, banks and their group companies are also subject to capital, liquidity, recovery and resolution planning and other requirements, in accordance with the principles of consolidated supervision. The framework for consolidated supervision is not applicable to non-banks (i.e. non-deposit-takers), such as technology companies, performing similar financial services activity.*

The resulting divergences in regulation may constitute significant regulatory obstacles or produce regulatory gaps, thereby impacting the level playing field for providers of the same services, and imposing additional costs for compliance with multiple regimes.

Therefore, market participants offering the same service or product should be regulated by rules that are truly activity-based and conceived according to the risks that the specific activities produce – in particular for end-users. That is, departing from the traditional institutions-based framework, the same regulations should apply regardless of whether the activities are led by an incumbent financial institution, BigTech or start-up (whether or not controlled by a financial institution). This principle should apply to all types of rules, including prudential rules, organizational requirements or conduct rules.

The similarity of the relevant activity should be considered by taking a functional view of its effect, for instance in terms of consumer risk and, therefore, the standards of protection needed. The same activities can still be subject to differing regulatory obligations where they do not entail the same risks, whether individually or in combination. Describing the risk that an activity creates is more complex, as this requires an assessment of all consequences of that activity in its broader context. If activities, albeit the same, entail different risks, they can be subject to different rules.

***Use case Payment services***

*Over the past decade, the payments sector in the EU has evolved rapidly. This evolution has been driven by changes in consumer preferences (the search for convenience) and supported by technological developments (e.g. online and mobile payments and contactless payment cards) and regulatory and oversight changes[82] intended to open access to payment services, facilitate faster payments, and promote greater choice for consumers. Notably, the PSD2 envisages new types of payment service provider[83] and, with a view to enhancing innovation and competition in the payments sector, requires account servicing payment service providers (ASPSPs) to share, subject to consent, customers' payment account information with other types of regulated third parties. Likewise, since the advent of e-money arrangements, new types of EU-wide payment schemes have appeared, ranging from SEPA credit transfers and direct debits, to instant payments and more recently tokenised payment arrangements.*

*As a result of these changes, the EU payments sector comprises a wide array of payments service providers and payment schemes with the value of electronic payments continuing to rise relative to other forms of payment (in particular cash).[84]*

*Looking ahead, newer technologies, for example distributed ledgers, smart contracts and AI, have the potential to further transform the sector. In particular, these technologies may help speed up payment processing times and generate cost savings and may further impact the structure of the sector.*

***Recommendation 14 – EU-level facilitation, including 'the sandbox'***

***The Commission and the ESAs should further assess the need to establish an EU-level 'regulatory sandbox', or similar scheme, taking account of the experience acquired in the context of European Forum for Innovation Facilitators.***

*Background*

In the EU, five national competent authorities have now established regulatory sandboxes with at least five more under development, and most competent authorities have established innovation hubs (together with 'innovation facilitators' – see box below).

[82] Directive 2007/64/EC (the first Payment Services Directive) (PSD1) and Directive 2015/2366/EU (the second Payment Services Directive applicable from 1 January 2018) (PSD2). Additionally, the Single European Payments Area (SEPA) was established, enabling EEA consumers, businesses and public administrations to make and receive cross-border electronic payments (credit transfers, direct debits and card payments) in euro with the same ease with which domestic payments are made.

[83] The PSD2 brings within the scope of regulation new types of payment services, namely account information services (AISPs) and payment initiation services (PISPs).

[84] Bank of International Settlements, *Shaping the future of payment* (2018) < https://www.bis.org/statistics/payment_stats/commentary1911.htm> | Accessed 25 June 2019

The ESA's joint report on innovation facilitators underlined the need for enhanced co-operation between the innovation facilitators.[85] As a result, the European Forum for Innovation Facilitators (EFIF) was launched in April 2019, with a view to bridging these national schemes and promoting a stronger dialogue on innovation-related issues in order to facilitate the adoption of common regulatory and supervisory stances. The EFIF can also be used as a means to promote greater coordination with innovation facilitators established in third countries – a point to be encouraged, bearing in mind the borderless nature of many technologies under consideration.

To guarantee a level playing field throughout Europe with regard to the instalment or use of sandboxes, building on the best practices set out in the ESA's joint report, the system of sandboxes should be further harmonized so that every national supervisory authority follows common principles and standards, while the rules and procedures are as streamlined and transparent as possible. This would guarantee a level playing field in terms of access to sandbox schemes and facilitate cross-border business, as firms would be have to conform to a common testing framework, thereby enhancing confidence in, and portability of, test outcomes to other European jurisdictions, and network effects by better and more formalised coordination between regulatory sandboxes. All market participants should be treated equally: irrespective of the size or degree of establishment on the market, innovators of all kinds should be able to apply without discrimination. If the business activities are not yet regulated, but might in future become a regulated activity, the sandbox participant and the sandbox program should help inform an assessment of whether or not this business needs to be regulated. In carrying forward this work, the Commission and the ESAs should leverage the expertise of EFIF members and, following application of the common principles and standards and experience acquired in the operation of the EFIF, should further consider the establishment of an EU-level regulatory sandbox.

Finally, the Commission and the ESAs should monitor the outcomes of sandbox testing in order to ensure that initiatives which have been successfully assessed are smoothly and rapidly transitioned outside this sandbox and that regulation or other standards, if necessary, are swiftly adapted accordingly.

[85] European Banking Authority, *ESAs publish joint report on regulatory sandboxes and innovation hubs* (2019) < https://eba.europa.eu/esas-publish-joint-report-on-regulatory-sandboxes-and-innovation-hubs> | Accessed 23 June 2019

***Innovation facilitators***

*Over the past 18 months there has been a rapid increase in the number of innovation facilitators established by supervisors in the EU. Typically these take the form of:*

*'Innovation hubs' which provide a dedicated point of contact for firms to raise enquiries with competent authorities on FinTech-related issues and to seek non-binding guidance on regulatory and supervisory expectations, including licensing requirements.*

*'Regulatory sandboxes' which are schemes to enable firms to test, pursuant to a specific testing plan, agreed and monitored by a dedicated function of the competent authority, innovative financial products, financial services or business models. Sandboxes may entail the exercise of levers for proportionality – but these are the same supervisory levers as are available outside the sandbox, and can be applied only in accordance with relevant EU and national law.*

*Although relatively limited experience has been acquired with the operation of the schemes, they show significant promise in bridging the industry and the supervisory community, as set out in the January 2019 Joint ESA report on regulatory sandboxes and innovation hubs[86].*

*For firms, innovation facilitators can enable access to dedicated supervisory resources with specialist expertise in innovative use of technology and support them in navigating the licencing/wider regulatory framework.*

*For supervisors, innovation facilitators can enhance visibility of technology-related developments. This enhanced knowledge can translate into a better understanding of opportunities and risks presented by innovations, which is helpful in addressing the inadvertent practical barriers to the goal of technological neutrality.*

*Currently the innovation facilitators operate on a national basis. Over time this could lead to barriers in knowledge-sharing (e.g. of technological developments), or the development of different regulatory and supervisory approaches to innovative use of technology across the Single Market. Recognising this risk, the ESAs set out in their report options to enhance cooperation and coordination between innovation facilitators.*

*On 2 April 2019, the European Forum for Innovation Facilitators (EFIF)[87] was launched further to the ESA advice.[88] The EFIF is intended to provide 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*

[86] European Banking Authority, *ESAs publish joint report on regulatory sandboxes and innovation hubs* (2019) https://eba.europa.eu/esas-publish-joint-report-on-regulatory-sandboxes-and-innovation-hubs Accessed 23 June 2019.

[87] https://esas-joint-committee.europa.eu/Pages/Activities/EFIF/European-Forum-for-Innovation-Facilitators.aspx

[88] V Dombrovskis, *FinTech Action Plan: Keynote speech by VP Dombrovskis at the inaugural event of the European Forum for Innovation Facilitators*, 2 April 2019.

*treatment of innovative products, services and business models, intended to boost bilateral and multilateral coordination.*

*This enhanced engagement between supervisors is intended to foster the development of a common regulatory and supervisory response through regular information exchange and discussion. It is also intended to help speed up the identification of any areas in which action may be needed to address risks to consumers, market integrity or financial stability, or to address recurrent obstacles or gaps impeding the scaling-up of FinTech across the EU.*

*Importantly, the EFIF can also provide a platform for supervisors to collaborate in responding to firm/group-specific questions about innovations and, for those with regulatory sandboxes, to agree where appropriate and, on a voluntary basis, joint testing arrangements, again supporting consistency in the supervisory responses to FinTech.*

---

## *End fragmentation, especially regarding KYC*

### ***Recommendation 15 – Uniform regulation***

***The Commission, in co-operation with the ESAs, should review the aspects of financial regulation that are currently subject to fragmented regulation and assess how to address them to ensure the highest possible uniformity across the EU in order to foster efficiency and competitiveness.***

*Background*

Regulatory fragmentation dents market efficiency in all kinds of contexts. Competitiveness of EU-based FinTech is vulnerable to divergent requirements. This is because the efficiency of technology-enabled financial services increases with market size. In other terms, regulatory fragmentation prevents the scaling of applications.

Currently, FinTech in the EU experiences fragmentation and the consequential hurdles to scaling up, for example, in the following areas:

- Differing KYC rules, including in relation to the acceptance of e-ID (see Recommendations 16 and 17);
- Differing consumer-facing and conduct of business rules (e.g. disclosure requirements, language requirements, complaints handling and financial promotions rules);[89]

[89] See further European Banking Authority, *EBA Report on potential impediments to the cross-border provision of banking and payment services* (2019) < https://eba.europa.eu/eba-calls-european-commission-take-action-facilitate-scaling-cross-border-activity> | Accessed 1 November 2019

- Differing rules on the format in which IBAN is accepted;
- Different understanding of who is a shareholder under the SRD.

Continuing fragmentation leads to a situation in which the benefits of the Single Market do not fully materialise for technology-enabled finance, as significant regulatory cost arises wherever providers are seeking to offer services in more than one jurisdiction. Addressing these issues would help remove frictions in the provision of services cross-border, strengthening the EU Single Market for financial services which, as a natural consequence, will enhance the global competitiveness of financial services regulated in the EU.

In addressing these issues the Commission should strive to achieve maximum convergence.

***Recommendation 16 – Fully harmonised KYC processes and requirements***

***The Commission, in co-operation with the EBA, should introduce legislation to fully harmonise the Know Your Customer (KYC) processes and requirements across the EU for obliged entities in the financial sector according to the AMLD with regard to identification and verification processes, as well as the mandatory collected set of data.***

*Background*

The Group considers divergences in KYC processes across jurisdictions to be the single most important example of fragmentation which harms the provision of services across borders using FinTech.

Level 1 regulation leaves significant national discretion regarding the implementation and application of the mandatory collected dataset of the identified person and the verification and identification process. As a consequence, one Member State might not permit the acceptance of an official ID of another Member State, or may require different forms of documentation (e.g. tax, utility bills etc.) in paper-based or digital formats, for KYC purposes.

Onboarding of new customers remains, as a consequence, a firmly jurisdiction-based process. Accordingly, firms seeking to provide services in more than one jurisdiction may need to adapt their compliance processes in each jurisdiction – a costly process, detrimental to the provision of cross-border financial services and a hindrance to the development and scaling up of, FinTech. To address these issues, the Group considers that KYC processes with regard to identification and verification should be fully harmonised.

***Recommendation 17 – Convergence in the use of innovative technologies for CDD purposes***

***The Commission and the EBA should take steps to achieve convergence in the acceptance, regulation and supervision of the use of innovative technologies for CDD purposes, including remote customer onboarding, and consider them on their respective merits, including through:***

- ***enhanced industry engagement and monitoring of market developments;***

- ***periodic updates of the Risk Factor Guidelines to support the use of these innovative technologies;***
- ***further guidance relating to reliance on third parties, including on issues relating to liability;***
- ***changes to Level 1 legislation (e.g. the AMLD), based on the advice of the EBA.***

***Recommendation 18 – Clarifying the capacity to re-use CDD data***

***The Commission, in cooperation with the EDPB and the EBA, should clarify the rights of data subjects to permit the use of data provided for CDD purposes and the outcome of identity verification for further identified purposes, where the data subject consents.***

*Background*

'Customer due diligence' (CDD) measures are designed to mitigate the risks of the financial sector being used for money laundering and terrorist financing[90]. CDD measures consist of a requirement for financial institutions to verify a customer's (and, where applicable, beneficial owner's and beneficiary's) identity on the basis of documents, data or information obtained from reliable and independent sources, to assess and, as appropriate, obtain information on the purpose and intended nature of the business relationship and transactions and to monitor both transactions and the business relationship. Traditional reliance on traditional paper-based documentation for customer identification purposes can give rise to problems in an online and remote on-boarding context.

Technological innovations facilitate remote, including cross-border, identification of new clients using, for instance, video conference or biometric verification. And new applications, for instance of DLT to facilitate the sharing of CDD information, or electronic registries (e.g. of beneficial owner information) could drastically reduce the cost of CDD.

In the EU, credit institutions and other financial institutions are subject to obligations to apply CDD measures in accordance with Directive (EU) 2015/849 (AMLD4).[91] Directive (EU) 2018/843 (AMLD5), once transposed into Member State legislation, will extend the list of obliged entities to virtual currency exchanges and custodian wallet providers.[92]

---

[90] On KYC processes, see Euro Banking Association, *Cryptotechnologies: improving Regulatory Compliance* (2018) < https://www.abe-eba.eu/epaper/epaper-EBA-Cryptotechnology-2018/epaper/EBA_Cryptotechnologies.pdf > | Accessed 2 July 2019; Financial Action Task Force, *International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation* (2019) < https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf > | Accessed 2 July 2019.

[91] See Articles 3(1) and (2) for the definitions of 'credit institution' and 'financial institution' of the DIRECTIVE 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EU .

[92] For a discussion about the application of AML/CFT requirements in the context of crypto-assets, see chapter 3 of European Banking Authority, *Report with advice for the European Commission on crypto-assets* (2019) < https://eba.europa.eu/eba-reports-on-crypto-assets > | Accessed 3 June 2019; The AMLD5 is required to be transposed into national law by January 2020. Further changes to the scope of AML/CFT

The AMLD is technologically neutral in the sense that it does not prescribe the precise modalities for CDD measures. Indeed, AMLD4 clarified that the absence of a customer is no longer, of itself, a high risk factor, and can be mitigated via certain safeguards such as electronic signatures. AMLD5 goes further[93] by recognising the use of electronic identification means more broadly, including relevant trust services as defined in Regulation (EU) 910/2014 (eIDAS Regulation[94]) – in effect recognising statements, credentials or electronic certificates under the eIDAS Regulation as a valid means of identity verification.

However, as the AML rules are based on a minimum harmonisation directive, Member States, in the context of the transposition of the Directive and for the purposes of implementing the risk-based approach, can include measures where necessary to mitigate the ML/TF risk, causing variations between the Member States. Neither AMLD4 nor AMLD5 set out in detail how obliged entities should apply CDD measures and, as a result, Member States' national frameworks vary (e.g. in terms of acceptable documentation for identity verification purposes, the form of that documentation (digital/paper-based), and thresholds triggering CDD measures for occasional transactions).

Although the recent modifications in AML legislation open the way for the development of digital solutions for CDD and the EBA and other ESAs have taken steps to foster a common understanding about the responsible and effective use of innovative solutions for CDD purposes,[95] fragmentation continues to exist. For example, Member States have adopted different approaches to CDD relating to, in particular:

- the documentation required for identity verification (e.g. passports, utilities bills, civic registrations, tax documentation) and format (acceptability of electronic copies vs physical copies);
- remote customer on-boarding (e.g. information requirements, supplemental measures for identify verification, such as video chat requirements);
- reliance on third parties for CDD (e.g. time restrictions on the use of non-face-to-face identification).[96]

---

requirements may be needed as a result of the changes to the FATF standards adopted in October 2018 (see further the EBA's report).; Maria Bergström, *The Global AML Regime and the EU AML Directives: Prevention and Control* [2018] Tha Handbook of Criminal and Terrorism Financing Law, Colin King ed.; Colin King and others, *The Palgrave Handbook of Criminal and Terrorism Financing Law*, Springer, 33-55

[93] Annex III in AMLD5, which sets out a non-exhaustive list of factors and types of evidence of potentially higher risk for the purpose of undertaking enhanced due diligence measures, is now changed to be more accommodating to digital ID solutions. It covers "non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities;

[94] The eIDAS Regulation is expected to help 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. European Commission, *FinTech Action Plan: For a more competitive and innovative European financial sector* (2018) < https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-109-F1-EN-MAIN-PART-1.PDF> | Accessed 2 June 2019.

[95] https://eba.europa.eu/esas-publish-opinion-on-the-use-of-innovative-solutions-in-the-customer-due-diligence-process

[96] AMLD4 allows institutions to rely on third parties (Article 26) to meet some of their CDD obligations. However, when transposing the Directive, some Member States have limited the use of third party reliance, for example, by requiring that third parties comply with the same requirements as those applicable domestically, or that an initial identification carried out by a third party is not older than, for example, 24 months.

The big challenge, from an EU perspective, therefore remains for digital CDD solutions to be compatible across borders. Until this fragmented national approach to CDD is addressed, technological innovation will be unable to release its full beneficial potential, as variations in national law can hinder firms from extending their services cross-border due to the complexities in navigating different national requirements and the increased compliance costs stemming from the need to put in place different systems and controls to satisfy these requirements. This cost represents a barrier to entry both for new entrants and for incumbents looking to extend the range of their financial services to consumers in other jurisdictions. As a consequence, whilst digital solutions make it easier than ever for firms to reach consumers in other jurisdictions, in practice national variations in CDD (and other conduct of business)[97] requirements pose a significant obstacle to the scaling up of activities.

For these reasons, the Group recommends the Commission and EBA take action to achieve convergence in the use and acceptance of innovative technologies for remote customer onboarding. The Group does not consider that harmonisation in this area would impede Member States in implementing a risk-based approach to ML/TF risk.

At the outset, this action should involve greater industry engagement to enhance monitoring of emerging technological solutions and market practices, and periodic updates to the EBA Risk Factor Guidelines to further enhance competent authorities' understanding of ML/TF risks associated with remote on-boarding and innovative technologies, and to promote a common approach to the acceptability of these solutions for AML/CFT purposes. The need for Level 1 (e.g. AMLD) amendments should also be kept under review.

Ideally, such rules should be enshrined in a Regulation instead of a Directive.

With respect to third party reliance, the AML Directive permits obliged entities to rely on third parties to meet CDD requirements, while stipulating that the ultimate responsibility remains with the obliged entity itself. The ability of financial institutions to trust CDD information gathered elsewhere via digital onboarding processes is therefore of paramount importance. However, because institutions remain ultimately responsible for meeting their CDD obligations even in a third party reliance scenario and lack comprehensive guidance in relation to reliance on third parties, not all institutions have chosen to make use of the possibilities afforded by this provision. The Group recommends that actions be taken, for example, in the form of EBA guidelines, to provide greater clarity in this area.

Finally, under existing EU law, there is a lack of clarity about the circumstances in which data provided for CDD purposes, and the results of identity verification, can be re-used for purposes other than CDD. In line with Recommendation 28**,** the Group recommends that the European Commission, in cooperation with the EDPB, take steps to clarify that this information may be used for purposes beyond CDD (i.e. 'other purposes'), where the data subject consents.

---

[97] On the importance of interoperability, European Banking Authority, *The EBA's FinTech Roadmap* (2018) < https://eba.europa.eu/eba-publishes-its-roadmap-on-fintech > | Accessed 4 June 2019; European Commission, *European Interoperability Framework – Implementation Strategy* (2017) < https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF > | Accessed 5 June 2019

***Recommendation 19 – Digital identity verification***

***The Commission, in consultation with the EBA and relevant authorities, should investigate potential models (including decentralised models) for efficient, robust and trusted digital identity verification. The findings should inform a future legislative strategy on common digital identity solutions in the EU.***

*Background*

Digital identity, i.e. the ability to provide or prove something about an individual, entity or device without the need to use physical documentation or checks, has the potential to provide significant value for consumers, businesses and for the economy as a whole.

From a firm's perspective, a digital identity framework enabling them to efficiently and securely prove a consumer's identity online, without the need for physical documents, would likely provide a significant boost for innovation across the economy, while simultaneously reducing the fraud levels and costs that industry currently incurs to manually prove consumers' identities.

The main potential advantages of digital identities are; improved onboarding, enhanced risk scoring (both credit and fraud) and data privacy considerations. The ability to enrich data with known identities can also help to improve AML/CFT controls. There is a huge opportunity for firms to provide a service that will become more important than ever in a world where identity and data attributes become extremely portable.

From a customer perspective, a true digital identity should be portable and reusable in the same way as a passport or identity card is today. Digital identities allow consumers to authenticate and legitimize themselves online. They can centrally log their information with a digital identity provider and make this information – after verification by the provider - available to third parties, for example when purchasing goods or services on the Internet.

There are several different models for identity verification (centralised,[98] federated[99] and decentralised[100]) and digital identity providers are often actors (such as financial institutions) that verify client identity for their own purposes, in particular during the process of onboarding clients, seeking to add value to the verified customer data they already hold. Banks and insurers, for example, are well placed to provide digital identity services as they acquire and verify relevant identity data in the context of the CDD process that they are obliged to perform. Other types of actor also typically hold detailed knowledge of their clients' identities, such as

[98] A user shares their personal information with the provider of a good or service (ORG) and trusts that entity to store and manage their information in a secure and reputable way. Examples:- Banks, Telecoms, Insurance.

[99] A user shares their information with an organisation that then acts as an identity provider (IDP) – i.e. they share that information with a third party with the consent of the user. The information shared with the third party may be self-attested or verified to a standard (e.g. Gov. UK Verify). This model may include multiple IDPs and relying parties adhering to a common set of legal, technical and verification standards.

[100] The user is able to collect digitally verifiable data attributes (credentials) provided by an IDP with whom they have an existing relationship. They are able to hold them remotely and share them with a relying party when they wish to (subject to IDP revocation). A distributed ledger allows a relying party to establish the validity of the attributes that have been signed and countersigned by the IDP and user respectively.

telecommunication companies. Social networks and mobile device manufacturers may also enter the market[101].

In view of the potential of these solutions to generate efficiencies in the digital identification process, the Group recommends the Commission (in consultation with the EBA and relevant authorities) investigate the different models with a view to bringing forward a legislative strategy for the acceptance of common digital identity solutions in the EU.

***Recommendation 20 – End default paper requirement***

***The Commission, in cooperation with the ESAs, should take steps to remove provisions of financial services law that require documentation to be provided, by default, to consumers in hard copy. This is without prejudice to the right of consumers to request information in this format.***

*Background*

EU financial services law includes a number of requirements for information to be transmitted to consumers in hard copy form.

For example, under Article 23 IDD and Article 14 PRIIPS, information to the customer shall be provided on paper or, if the consumer agrees, on a durable medium other than paper or by means of a website. PRIIPs Article 14 provides that paper "should be the default option" where it is a "face-to-face" distribution. These requirements aim to enhance consumer protection by ensuring that retail customers have the necessary access to information that would allow them to make informed decisions, and that the format of information is appropriate for the channel by which a service or product is being transacted.

However, the requirement for 'paper by default' is difficult to reconcile with the idea of an increasingly digitalised market. Cost-efficiencies arising from technological innovations may depend on being able to process data digitally throughout the entire process.

At the same time, there is evidence that consumers pay less attention to information provided digitally than they would pay to information provided on paper. This extends to the question of whether the requirement to acknowledge receipt or having understood the information changes anything at all. Hence, the opportunity should be taken to develop new concepts that allow the use of potential efficiency gains, while at the same time maintaining, or even improving, effectiveness of providing information to retail clients.

For this reason, the Group recommends removing requirements (in EU and relevant national law) that require information to be transmitted in all cases to consumers in hard copy, whilst:

- preserving the requirement to provide information in specified formats in some cases (e.g. for the visually impaired), as the removal of such requirements could risk

[101] Device providers and initiators of private, global 'currency' systems have also announced the integration of ID solutions.

exacerbating the financial exclusion of some consumers. and the rights for consumers to request information in this format where preferred;

- considering new requirements to ensure that consumers receive appropriate, and readily digestible, information in line with their needs.

## *Access to infrastructures*

***Recommendation 21 – Participation in clearing and settlement systems***

***The Commission, in cooperation with the ESAs and the ESCB, should evaluate the need to revise the Settlement Finality Directive to allow for the participation in clearing and settlement and payment systems of any type of regulated financial institution, on the basis of appropriate risk-based criteria.***

*Background*

Financial market infrastructures (FMIs) are critical components of the financial system. They include payment systems, central securities depositories, securities settlement systems and central counterparties. Given the systemic nature of FMIs, access is restricted on the basis of risk-based considerations, laid down in relevant EU legislation (SFD, MiFID, EMIR, CSDR, and the SIPS Regulation).

Currently, EU law leaves scope for different national approaches governing access to FMIs. In particular, due to different transpositions of the Settlement Finality Directive (SFD), the ability of non-bank payment institutions (e.g. e-money institutions) to directly access designated payment systems varies between different EU jurisdictions.

Having regard to this, a review of the SFD to explicitly allow for and fully harmonise participation of non-banks to designated clearing, settlement and payment systems should be envisaged, as long as such participation is based on objective risk-based criteria (e.g. taking into account considerations such as operational resilience and risk management).

***Recommendation 22 – Access to platforms***

***The Commission should introduce rules to ensure that large, vertically integrated platforms do not unfairly discriminate against downstream services that compete against their own similar services.***

*Background*

The emergence of platform business models combining different types of financial and non-financial products and services poses both opportunities and challenges. On the one hand,

digital platforms offer consumers convenience and can facilitate the provision of services cross-border. On the other hand, unless appropriately regulated, they can pose new forms of risk (e.g. cyber security and operational resilience). Additionally, platforms can pose efficiency problems for the wider market. For example:

- large technology companies with access to significant social media, search history and other data, may leverage their preferential data access to enter the market for financial services, at the same time benefiting from access to data such as payment account information, as facilitated pursuant to the PSD2. Without appropriate regulation, these companies could emerge as oligopolies which effectively lock customers into their platforms and promote only their vertically integrated services, thereby leveraging their dominance over data access to support their business in downstream markets;
- providers of smartphone operating systems may not provide access to the relevant devices' NFC interface for competing payment applications. This can represent an obstacle to innovation because access to the NFC interface is necessary to enable fast and easy use of mobile payments. As a consequence, mobile payment on the relevant devices can only be offered by the provider of the operating system;
- some providers do give access to devices or software, but under conditions that can create inefficiencies, such as a prohibition to use other consumer interfaces. Some providers may leverage their dominance in one market to boost their performance in different markets by demoting rivals' financial products and services in search engine results.

Once the vertical 'silo' is established, it becomes very difficult to compete with the dominant provider's services or products. While abuse of a dominant position is a matter of competition law, the latter is reactive instead of proactive as an investigation is required which needs to establish a competition abuse has occurred, hence, it may not effectively prevent the issue from arising, leaving consumers and other market participants exposed to a dysfunctional market and the detriment that follows, long before authorities are in a position to intervene on the basis of competition law.

For this reason the Group recommends that the Commission take action to introduce *ex ante* rules to prevent large, vertically integrated platforms from discriminating against product and service provision by third parties.

## *Limitation of scope of business*

### ***Recommendation 23 – Framework for P2P insurance***

***The Commission, in cooperation with EIOPA, should evaluate the need for a framework for the regulation of P2P insurance.***

*Background*

The innovative use of technology is having a significant impact on the sale and distribution of insurance products and services. For example, in-person communications are being increasingly replaced by digital interactions and technologies, in particular AI, are increasingly helping to simplify interactions with clients. At the same time, digitalisation of sales and distribution are enabling disintermediated sales through the internet or mobile phone applications and new market players, such as comparison websites, have quickly gained a prominent role in the sale and distribution of certain lines of business.

European insurance legislation does not provide a definition of what constitutes 'insurance'. Art 13(1) Solvency II states that 'insurance undertaking' means a direct life or non-life insurance undertaking which has received an authorisation. The IDD, which is a minimum harmonisation directive, provides a broad definition of what should be understood by insurance distribution (Article 2(1)(1)). The definition of insurance is often (not always) included in national legislation or case law, and therefore there is no common EU approach in this regard, which can also lead to diverging views of what is P2P insurance or other types of insurance-related products and services.[102]

From a regulatory perspective, and following an activity-based approach, it can be argued that there are three different types of P2P insurance business model: a) P2P insurance sold directly through a licensed insurer; b) P2P insurance sold via a licensed/registered insurance intermediary backed by a licensed insurance undertaking (e.g. an intermediary (or agent) may branch out to broker (multiple underwriters used) or an MGA (which takes a much higher share of the insured activity and risk), and c) service providers/platforms acting solely as administrators for risk sharing groups, without an underlying insurance carrier and without performing insurance distribution activities, in so far as the risk sharing is deemed not to be insurance.

While there is a clear applicable legal framework for the first two types of P2P insurance business models, this is not so clear in the case of service providers/platforms purely acting as an administrator for risk sharing groups. It is also debatable whether Solvency II and IDD are adapted to all new types of P2P insurance business model. One could argue that the low penetration of P2P insurance is due to a lack of clarity as to the application of the legal framework for these types of business models.

In the opinion of the Group, an initiative covering insurance following concepts similar to the European Commission's crowdfunding legislative proposal[103] could facilitate the penetration of P2P business models in insurance, facilitating the access to alternative risk management tools for consumers or offering them a wider range of choices and specifying governance and disclosure elements, so that consumers understand in what kind of business they are engaging.

---

[102]European Insurance and Occupation Pensions Authority, *Report on Best Practices on Licencing Requirements, Peer-to-Peer Insurance and the Principle of Proportionality in an Insurtech Context* (2019) < https://eiopa.europa.eu/Publications/EIOPA%20Best%20practices%20on%20licencing%20March%202019.pdf > | Accessed 2 November 2019

[103] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-5288649_en

However, the protection needs of insurance customers are different, arguably higher, than those of crowdfunding investment models, in particular regarding certain types of insurance products.

***Recommendation 24 – Proportionate restrictions on non-core business***

***The Commission, in cooperation with the ESAs and the ESCB, should consider the impact of existing activities restrictions for financial institutions' non-core business, to determine whether these restrictions remain proportionate and, if so, whether the restrictions are consistently applied having regard to the need to maintain a level playing field.***

*Background*

Current EU financial services law typically envisages that financial institutions may carry out specified core activities in accordance with the applicable licence or registration regime. However, limitations may exist for non-core business (albeit these do not prevent institutions from establishing group companies to carry out such business). For example:

- Article 18(1)(a) and (b) of Solvency II limits the types of products and services that insurers can offer to the insurance business or activities arising directly therefrom. Insurers may, for example, be constrained from cross-selling products containing on the one hand a pure insurance products combined with other products or services such as fire alarms or theft alerts for buildings or cars, coaching about driving styles via apps, e-medicine services, etc. requiring a fixed contribution from the customer;
- credit institutions are permitted, pursuant to their licence status, to carry out specified regulated financial services listed in Annex I to the CRD and other business activities unless expressly prohibited as a matter of national law or restricted as a result of the exercise of supervisory powers;[104]
- PSD2 envisages that entities carrying payment services activities of a kind set out in Annex I to the Directive may carry out other business activities, albeit competent authorities may require the establishment of a separate entity for the payment services business in specified cases (Article 11(5)).

As a result of these and similar restrictions, financial institutions may be prejudiced compared to firms outside the regulated financial sector, both in their capacity to innovate and to carry out other business activities. For instance, BigTech firms can cross-sell insurance and other financial products through their online platforms.

In view of the increased digitisation of financial markets, these limitations should be reviewed to assess whether they remain proportionate. In carrying out this review, particular regard

[104] For example, see the discussion in the context of the EBA's January 2019 report on crypto-assets (see chapter 4): https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1

should be paid to cross-sectoral considerations, in order to ensure a level playing field between different types of actor in the financial sector, including BigTech.

# Access to data

The worldwide data economy is characterized by an ecosystem of different types of market players competing and collaborating to generate additional value. Increasingly, it is the ability to access data that provides market players with market power – a key element in the EU's global competitiveness going forward.

The provision of technology-enabled financial services is highly dependent on data. Finance and banking are heavily reliant on information as part of the everyday business decision-making processes, from granting loans to managing investment portfolios. The financial sector generates vast amounts of data, which resides within financial institutions and does not circulate. The arrival of PSD2 will to some extent change that (i.e. with regard to payment account information). Additionally, firms seeking to enter the financial sector may leverage other forms of information (e.g. social media information). In addition, new technologies such as AI and machine learning are creating new possibilities for the transformation of vast and granular amounts of data into valuable information.

The blurring of different sectors and sources of information in the context of the provision of financial services will have disruptive impacts, as those companies that have the capability to transform data into valuable information and enrich it with other sources of data e.g. through use of social networks, will have a competitive advantage.

As one of the distinctive aspects of European law, the protection of natural persons in relation to the processing of their personal data is recognised as a fundamental right. Both the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of their personal data. The GDPR, which has been in application since 25 May 2018, is an ambitious framework that harmonises data protection rules in the EU and empowers individuals by putting them in a position of control over their data, notably by reinforcing their rights, while also posing a number of challenges for the industry. It appears that the GDPR now serves as a guiding text for new data protection regulations in various jurisdictions, such as in Brazil (Lei Geral de Proteção de Dados), India (Indian Personal Data Protection Act) and California (California Consumer Privacy Act), which is particularly relevant for the development of the data economy.

Personal data may, according to the GDPR, be processed only in accordance with certain general principles (e.g. transparency, purpose limitation and data minimisation) and on the basis of a legitimate ground, respecting certain rights of the data subject, such as the right to be informed or the right to be forgotten.

Depending on the origin of the personal data, one can distinguish between declared data (data actively and knowingly provided by the customer), observed data (created through customer activity); and inferred data, which is created by the data controller on the basis of the data 'provided by the data subject' e.g. data validation, analysis, profiling, etc.

With respect to non-personal data, the Regulation on the free flow of non-personal data establishes a framework for the free movement of non-personal data in the EU, banning

unjustified restrictions related to requirements imposed by public authorities on the location of data for storage or processing.

***Recommendation 25 – GDPR and new applications of technology***

***The EDPB should issue guidance on the application of the GDPR and other relevant legislation, in relation to the innovative use of technology in financial services, including the use of:***

- ***DLT/Blockchain, in particular how to satisfy the requirement for erasure, for example, using encryption;***
- ***Artificial Intelligence, in particular addressing the issue of specificity of consent.***

*Background*

In the context of the data driven economy, it is essential that firms can use and experiment with different sources of information in combination with, in particular, AI. However, currently, firms may be held back due to uncertainties about how to comply with data protection rules when using blockchain, AI and certain other technologies. For example:

- In the context of storing personal data on private and public Blockchains, it is unclear how compliance with requirements to delete personal data (in the context of the 'right to be forgotten') can be achieved in an infrastructure that is characterised by immutability of records. The French data protection authority (CNIL) acknowledged that some encryption techniques can potentially be considered erasure if the respective keys are destroyed in the sense of the GDPR.[105] There may also be other technical ways, such as off-chain storage, to achieve the same result as an erasure. However, at the EU-level, there is uncertainty in the market as to whether any of the various methods would be considered compliant;
- It is difficult to obtain consent of the data subject for the use of their personal data for the purpose of AI experimentation. The purpose limitation principle makes it difficult to rely on the validity of any consent given. Further, the data minimisation principle requires deletion or anonymization of all data that is not necessary for the specific purpose for which it was collected. 'Necessity' is interpreted narrowly and the data minimisation principle limits all use of data, including where there is consent. However, this principle is difficult to apply in the context of data experimentation, unless experimentation actually takes place, by which point in time it would be too late to validly obtain consent;
- Finally, in practice, the situation is further complicated by the fact that personal and non-personal data are often difficult to separate. This leaves the options of either

[105] Commission Nationale Informatique & Liberte, *Premier element d' analyse de la CNIL* (2018) < https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf > | Accessed 10 June 2019

anonymising the whole dataset at significant cost or submitting it to the rules applicable to personal data, which makes it useless for experimentation purposes. In some non-EU jurisdictions, such restrictions do not exist as a consequence of lower standards of protection.

In order to address these issues and promote a consistent approach across the EU, the EDPB should provide detailed guidance to support the industry to comply with obligations under the GDPR when utilising innovative technologies. Other issues where guidance would be welcome include:

- the distinction between testing data and training data and the implications for data processing (e.g. confirmation that Article 5(1)(b) GDPR research exemption would be available where data is being used for training only and where no decisions are being taken);
- the scope for relying on 'privately funded research' in the context of data use and experimentation in the context of AI use and other technologies;
- the application of Article 6(4) GDPR 'not incompatible with original purpose'.

***Recommendation 26 – Regulatory Dialogue***

***The regular dialogue between the European Data Protection Board, the European Forum for Innovation Facilitators, national data protection authorities, national and EU competition authorities, national and EU financial regulators and financial supervisors and firms should be extended, with a view to keeping under review the practical application of relevant EU legislation concerning the processing of data (in particular GDPR and PSD2), taking account of technological developments within and beyond the financial sector. The objectives of this dialogue should be to:***

- ***enhance knowledge-sharing about new technologies;***
- ***share experiences and promote a common approach to the regulatory and supervisory approach to the practical application of relevant EU legislation concerning the processing of data;***
- ***provide where appropriate clarification of or guidance on relevant EU legislation concerning the processing of data in a form that is publicly accessible.***

*Background*

Innovative technologies are being used in a wide range of contexts within and outside the financial sector. Keeping track of market developments, particularly in a context where sectoral distinctions are becoming less and less relevant, and maintaining a fit-for-purpose overall scheme of regulation and supervision in the EU represents a significant challenge, including in the context of data protection.

For this reason, the Group urges enhanced multi-disciplinary coordination between relevant authorities. In particular, the Group calls on the EDPB to step-up its dialogue with the industry,

those authorities with closest proximity to the application of technologies in the financial sector, including via the EFIF, and relevant competition and data protection authorities. This enhanced dialogue should be specifically aimed at promoting knowledge-sharing about specific use cases, greater consistency in the application of EU data protection legislation in the context of those use cases (e.g. the use of DLT), and facilitating the provision, on a more timely basis, of clarifications or changes to the regulatory framework as may be required taking account of these developments.

***Recommendation 27 – Access to and processing of non-personal data***

***The Commission should develop measures to provide legal certainty on the access to and processing of non-personal data by different stakeholders. In preparing these measures, the Commission should assess the need for an EU-level supervision and enforcement mechanism and ensure consistency across the EU.***

*Background*

Whilst the EU has the GDPR which sets out a comprehensive framework regarding access to and processing of personal data, there is currently no similar framework for non-personal data (albeit the regulation on the free flow of non-personal data aims at removing obstacles to the free movement of non-personal data across Member States and IT systems in the EU).

Non-personal data is valuable, and at present, there is no regime clarifying the rights of data subjects to determine who and how data may be accessed and processed, in particular for the purposes of porting it to another service provider who could equally generate value from it. This may create inefficiencies. Indeed, the exchange of data is crucial for new business models. Against this background, the Group considers that the Commission should take steps to provide clarity, balancing the need for data subjects to have clear rights with regard to access to non-personal data whilst recognising the opportunities and costs for data controllers in terms of administering any new arrangements.

***Recommendation 28 – Data sharing***

***The Commission should introduce rules to ensure that a user of digitally enabled products or services has the possibility to share seamlessly, securely and in real-time with other market participants of their choice the data that the providers of those products or services have observed on them. These rules should support user control and data-driven innovation by ensuring sharing is easy, secure and effective, for example by mandating the use of standardised sharing interfaces.***

*Background*

Data is recognised as key to both users and the providers that they engage with; in particular, its careful management is needed to protect individuals' privacy and its use is central to the

creation of digital products and services. However, users (whether individuals or firms) have little effective control over the data that they produce when engaging with goods and services and capture little of the economic value that it generates, while European firms often have limited access to data that could allow them to compete more effectively and innovate in the digital economy.

At the same time, through the large scale of products and services offered across multiple marketplaces and their internal Big Data analytics, large operators of the big digital platforms such as Google, Amazon, Facebook, Apple and soon Baidu, Alibaba, Tencent already have/will soon have a significant amount of information about European customers (i.e. social network, place of residence, composition of the family, spending patterns, purchasing habits).[106] However, there is no obligation on the operators to share this information on a real-time basis with others on the instruction of the user. This leads to an asymmetric position in the market because these operators can benefit from access to payment account information required to be shared by banks and other payment institutions payment account providers in accordance with PSD2.

Indeed, PSD2 has set a precedent for user-driven data sharing under the limited scope of transactional payments account data. The benefits of PSD2 are that the data sharing happens in real-time and favours interconnectedness through APIs, hence facilitating innovation from the recipient side.

Potentially significant added-value could be provided to users if their non-financial data, e.g. search data, or social media data, were accessible by other firms, subject to their consent. In particular, this could enhance competition in the financial sector by levelling the playing field between different types of market participant via access to data. Additionally, widening access to data and reducing market concentration risk can help mitigate potential new threats to financial stability emerging from the entry of BigTech in the financial sector.[107]

In view of the breadth of relevant information, the Group considers that the necessary regulatory scheme should be developed on a horizontal basis, rather than on an activity- or sector-specific basis – and ensuring a high degree of security in the context of data-sharing.

---

***Examples:***

*1. Rewarding the driving behaviour of insurance clients could be further developed by technical standard options for access to in-vehicle data like mileage, speeding, time, geolocation, claims etc. This would require that the insurer has access to data from e.g. sensors in connected cars.*

*If only the car manufacturer has access to the information collected by the sensors, it would give the car manufacturer a negotiating monopoly and the ability to charge for access. It is therefore essential to empower customers to*

---

[106] For further background on the role and potential role of BigTechs in the financial sector, see: https://www.fsb.org/2019/12/fsb-reports-consider-financial-stability-implications-of-bigtech-in-finance-and-third-party-dependencies-in-cloud-services/

[107] Ibid.

*choose from a wide variety of service providers, instead of allowing a data monopoly for the benefit of car manufacturers.*

*2. Data sharing could be used to help meet administrative requirements in "life events" such as births, marriages or deaths as a way to notify service providers and relevant organisations so they can update records.*

*3. Additional information from a user about their energy use and building details could be used to offer tailored green loans.*

*4. Risk scoring could be improved by taking into account new factors in risk models, increasing access to credit in underserved markets, such as SME lending.*

# Financial inclusion and ethical use of data

***Recommendation 29 – Financial inclusion and exclusion***

***The European Commission, in cooperation with the ESAs, should monitor and have regard to the impact of the increasing use of technology-driven financial services on our society and, where significant issues arise, should take action to:***

- ***promote the use of those technology-driven financial services as a means to address financial inclusion;***
- ***prevent the use of those technology-driven financial services in ways that exacerbate financial exclusion or causes unfair discrimination.***

*Background*

FinTech, in its many forms, can serve as a tool to help promote financial inclusion,[108] by:

- providing new means for consumers to access financial services;
- enabling new, or cheaper, financial products and services;
- facilitating the provision of more tailored financial products and services;
- supporting cheaper and more sophisticated processes for credit-scoring and customer due diligence/KYC.

FinTech applications enable access to financial services via smartphones, online banking and online marketplaces, thereby radically changing the way in which many consumers use financial services, allowing access any time anywhere. The widened range of possibilities to access financial services enhances choice for consumers with such devices. Additionally, these kinds of applications and platform aggregation services can improve consumer visibility of their assets and liabilities and help consumers control their finances.

---

***Use case: Smart advice***

*'Smart advice' comprises all activities that use algorithms to provide insights and recommendations that help users manage their finances or make decisions that involve money, based on their behaviours and specific characteristics.*

*Currently many smart advice tools involve a degree of human intervention. However, it is anticipated that the predictive capabilities of these*

---

[108] European Parliament, *Report on FinTech: The influence of technology on the future of the financial sector* (2017) < www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.html > | Accessed 7 July 2019; European Commission, *FinTech Action plan: For a more competitive and innovative European financial sector* (2018) < https://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0001.02/DOC_1&format=PDF > | Accessed 7 July 2019; European Banking Authority, *EBA publishes its Roadmap on FinTech* (2018) < https://eba.europa.eu/eba-publishes-its-roadmap-on-fintech> | Accessed 7 July 2019

*technologies will improve, as will the level of automation, enabling more sophisticated advice strategies and customisation.*

*There are also expectations that the accuracy of predictions for a wide range of investment profiles, ranging from consumers to institutional investors, will improve, while costs decrease.*

---

FinTech may also improve competition, facilitating the market entry of firms offering more targeted or tailored financial products (e.g. payment solutions not requiring access to a traditional bank account; peer-to-peer lending platforms, etc.), equally resulting in wider choice for consumers and businesses.

FinTech may also lower the cost of financial services, e.g. through automated, and therefore cheaper, CDD processes that allow wider data sets and sources, allowing customers with no traditional credit record to access financial services, or through automated investment brokerage services. On the assumption that these cost savings are passed on to consumers, this may also facilitate access to, and choice of, financial services, as they become more affordable.

Although innovation in the financial sector is typically viewed as contributing a net positive towards addressing the issue of financial exclusion, it is important to remain mindful of risks that may exacerbate the problem.

First, not all consumers have access to electronic devices such as computers and smart phones. As the financial world becomes increasingly digitalised, societies need to ensure that these consumers are not left behind. This means that public authorities and the financial industry should continue efforts to promote digital inclusion in parallel with efforts to provide other means to access financial services for those who may not have capabilities to use the internet or card- or mobile-based payment solutions. In this context there is a tension between the need to preserve multiple means to access financial services and pure market efficiency. ATMs and bank branches in rural areas are a case in point, where the societal damage of not having them must be balanced against the cost implications. 'Digital only' business models so far seem to be immune to such arguments. It is a genuine policy challenge to take into account societal expectations for market participants, the range of potential business models and the need to preserve a level playing field.

Second, it has been argued that continuously evolving choices, and increased competition may lead to greater exclusion because those consumers who are not able to keep up with market innovation, or lack financial education, are left behind and can transact only on less favourable terms.

Third, it is vital that high standards of consumer protection continue to exist, regardless of the provider or means of provision of financial services, so that consumers do not face exploitation, unfair discrimination, detriment or prejudice as a result of the application of involving the novel use of technologies. This entails a multi-dimensional policy response including elements such as:

- the need for accessible and clear disclosure of consumers' obligations, rights and risks in relation to financial products and services;

- frameworks to ensure the ethical application of AI solutions, particularly in the context of credit scoring and robo-advice, the core elements of which rest on explainability or interpretability of automated decisions (see Recommendation 1), and the ethical use of data (see Recommendation 30);
- accessible and visible complaints handling and redress procedures should things go wrong (in particular, high levels of clarity as to which procedure applies in relation to products and services provided cross-border); and
- improved financial education and literacy.[109]

Overall, the causes of and solutions to financial exclusion are complex and FinTech is not and cannot be the silver bullet. However, the opportunities presented by, and potential risks of, FinTech should be kept constantly under review to ensure that the benefits of these technologies can be catalysed into important efforts to address financial exclusion.

---

***Use case *: Credit scoring***

*Credit-scoring describes the process of assessing the creditworthiness of a borrower based on statistical models. Credit scoring can be used as one of the criteria applied in decision-making processes regarding the provision of financial services, in particular consumer credit and mortgages. Where the credit scoring is the only criterion used in that decision, the process is tantamount to the actual decision to grant a loan.*

*Banks traditionally rely, for the creditworthiness assessment of their clients requesting a loan, on "hard data", i.e. objective and easily verifiable data, such as clients' credit history (e.g. number and types of loan previously requested, re-payment delays, etc.), income and net-worth or, in case of entrepreneurs, balance sheet and business plan. This data has traditionally been evaluated by a relevant employee of the lender.*

*New technologies, in particular AI, machine learning and Big Data are understood to offer the potential for a broader, deeper and faster analysis of large data sets, including "soft data" (e.g. harvested from social media) relevant to the assessment of creditworthiness. As such, they purport to offer a more accurate prediction of the credit risk posed by the person seeking funds.*

*This has the potential to offer benefits for consumers and businesses seeking credit, as greater accuracy may lead to the provision of more suitable and tailored products. For lenders, these solutions can help protect from credit risk and fraud, reduce the cost of the credit assessment process, foster the development, distribution and monitoring of products, and enable better consumer/client interaction. Indeed, over time, these solutions could displace human intervention in the process presenting significant cost savings. In light*

---

[109] Organization for Economic Co-operation and Development, *G20/OECD INFE Policy Guidance Digitalisation and Financial Literacy* (2018) < www.oecd.org/daf/fin/financial-education/G20-OECD-INFE-Policy-Guidance-Digitalisation-Financial-Literacy-2018.pdf > | Accessed 7 July 2019

*of these potential benefits, AI, Big Data and machine learning solutions are being increasingly piloted and rolled-out in the financial sector.*

***Recommendation 30 – Ethical use of data***

***The Commission, should, in cooperation with the ESAs and the EDPB, develop guidance to assist financial institutions in the ethical use of data in the context of the provision of financial services.***

*Background*

Leaving aside issues of financial exclusion (Recommendation 29) and 'black-box' biases (Recommendation 1), there is still need for a further guidance in relation to the ethical, in particular transparent and fair use of data, in the context of the provision of financial services.

Questions regarding the fair and transparent use of data can be considered in three ways.

First, the provenance of data**:** financial institutions utilise a wide, and increasing range of data sources in the context of the provision of financial services[110]. These sources include client-sourced data such as names, addresses, identification and employment records, third party data (e.g. credit reference agencies), and may include social media data. This enables providers of financial services, e.g. lenders or insurers, to position themselves more accurately in respect of their retail or wholesale counterparty or in respect of the market as a whole. As a consequence, risks and opportunities will be more accurately predictable. However, the use of non-client-sourced data, especially data harvested from the internet and social media, may be unvalidated and potentially subject to manipulation, such as reviews and 'likes'. In addition, data may be collected with reference to parameters which could be regarded as unfair, for example counting in data of family, friends and colleagues of the relevant data subject.

Second, the use case: some forms of data may be more or less relevant to a decision-making process and some may induce bias or give undue weighting to a particular source or type of data. Accordingly, the notion of fairness should be considered by reference to the specific context in which the data is being applied (e.g. credit scoring).

Third, the availability of data: some consumers may or may not be able to provide certain forms of data (e.g. some consumers may not subscribe to social media or may not have, for example, credit card accounts) but these consumers should not be disadvantaged in their access to financial services. Therefore, fairness should also be considered in this light and policy-makers will need to make difficult choices taking account of new types of available data (e.g. whether

[110] See Dirk Hovy and Shannon L. Spruit, *The Social Impact of Natural Language Processing*, https://www.aclweb.org/anthology/P16-2096.pdf and Sandra Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioural Advertising*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388639

the use of a fitness tracking device can be considered to be a permissible pre-condition for access to health insurance).

For these reasons the Group recommends the development of guidance on the ethical use of data in the context of the provision of financial services. This may include some elements that are common across the sector and some more tailored sector or service-specific measures (e.g. in the context of insurance concepts such as 'mutualisation', 'solidarity', 'causality' and 'actual fairness' need to be considered).[111]

[111] See also Philip Alston, *Extreme poverty and human rights* (2019) < http://www.statewatch.org/news/2019/nov/un-report-digital-welfare-states-10-19.pdf> | Accessed 6 November 2019.

# Conclusion – Establishing priorities in regulating FinTech

The Group applauds the European Commission's recognition of the transformative potential of FinTech and the work to-date by the Commission and the ESAs in accordance with the March 2018 FinTech Action Plan.

In the next phase of work, the Group recommends a doubling-up of ambition and effort to establish a truly accommodative approach to FinTech in the EU.

FinTech is evolving rapidly. As it is piloted, it is demonstrating its capacity to deliver greater choice and improved efficiencies in the provision of financial products and services. It is vital that policy makers recognise that potential and take steps to ensure that the financial sector is able to keep pace with these rapid and ground-breaking changes.

The Group acknowledges that there are important synergies with the EU's Digital Single Market Strategy[112], the Consumer Financial Services Action Plan[113], and the Capital Markets Union[114] and recommends a multi-dimensional approach to foster a truly accommodative framework for FinTech in the EU.

Such a framework should enable the benefits of FinTech to be leveraged, whilst maintaining high standards of consumer protection, market integrity and the stability of the EU financial system. Delivered well, it should also have the effect of protecting and enhancing the attractiveness of the EU as a global financial centre.

The Group sets out in this far-reaching report a considerable number of recommended actions, ranging from the monitoring of market developments and emerging opportunities and risks, the clarification of the applicability of (or where appropriate adaptation of) existing EU regulation, to the introduction of new EU law.

In some cases, the Group identifies the need for immediate and bold policy action. In particular, the Group identifies several areas where industry is being held back in its capacity to leverage available technology by the absence of clear regulation (in particular, in the area of crypto-assets) and also notes that markets may establish practices which are difficult to change subsequently (e.g. around the use of data), pointing to the need for ex ante bold thought leadership and policy action.

Taking these factors into account, the Group has reviewed the recommended actions and would wish to highlight in particular the importance of the following recommended measures:

- The explainability and interpretability of technology, especially AI, as measures to protect consumers and businesses and facilitate supervision, or to meet supervisory expectations (Recommendation 1);

[112] https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market

[113] https://ec.europa.eu/info/publications/consumer-financial-services-action-plan_en

[114]https://ec.europa.eu/info/business-economy-euro/growth-and-investment/capital-markets-union/capital-markets-union-action-plan_en

- The creation of a regulatory framework built on the principle that activities that create the same risks should be governed by the same rules, with a view to ensuring adequate regulation and supervision and maintaining a level playing field (Recommendation [13]);
- The ending of regulatory fragmentation, especially in the area of customer due diligence/KYC, as an important step towards creating a level playing field (Recommendations 15-17);
- Preventing unfair treatment of competing downstream services by large, vertically integrated platforms, in order to strengthen innovation and maintain consumer choices (Recommendation 22);
- The strengthening of the framework for access to, processing and sharing of data, in order to promote innovation and competition and establish a level playing field amongst actors (Recommendations [27] and [28]).

The Group stresses that the aims informing these and all other Recommendations are best pursued by regulation that is neutral, in the sense that it does not differentiate between the different technologies that can potentially be used to provide a service, offer a product or perform a function. The Group further believes that international cooperation in setting relevant standards, ideally leading to interoperability, is crucial in this exercise.

# Glossary of Acronyms

| | |
|---|---|
| AI | Artificial Intelligence |
| AIFMD | Alternative Investment Fund Managers Directive |
| AISP | Account Information Service Provider |
| AMLD | Anti-Money Laundering Directive |
| ANN | Artificial Neural Networks |
| ASPSP | Account Service Payment Service Provider |
| BBN | Bayesian Belief Network |
| BRRD | Bank Recovery and Resolution Directive |
| BWUD | Bank Winding Up Directive |
| CDD | Customer Due Diligence |
| CFT | Counter Financing of Terrorism |
| CNIL | Commission Nationale de l'Informatique et des Libertés |
| CRD | Capital Requirements Directive |
| CRR | Capital Requirements Regulation |
| CSDR | Central Securities Depositories Regulation |
| DL | Deep Learning |
| DLT | Distributed Ledger Technology |
| EBA | European Banking Authority |
| EBPB | European Data Protection Board |
| ECB | European Central Bank |
| EFIF | European Forum for Innovation Facilitators |
| EIOPA | European Insurance and Occupational Pensions Authority |
| EMIR | European Market Infrastructure Regulation |
| ESAs | European Supervisory Authorities |
| ESCB | European System of Central Banks |
| ESMA | European Securities and Markets Authority |
| ETF | Exchange-Traded Fund |
| FCD | Financial Collateral Directive |
| FMI | Financial Market Infrastructure |
| GBN | General Bayesian Network |
| GDPR | General Data Protection Directive |
| GFIN | Global Financial Innovation Network |

| | |
|---|---|
| HFT | High frequency trading |
| IBAN | International Bank Account Number |
| ICO | Initial Coin Offering |
| IDD | Insurance Distribution Directive |
| InsR | Insolvency Regulation |
| IoT | Internet of Things |
| KYC | Know-Your-Customer |
| MiFID | Markets in Financial Instruments Directive |
| ML | Machine Learning |
| MTF | Multilateral Trading Facility |
| NFC | Near Field Communication |
| NLP | Natural Language Processing |
| PISP | Payment Initiation Service Provider |
| PRIIPS | Packaged Retail and Insurance-Based Investment Products |
| PSD2 | Payment Services Directive 2 |
| OTC | Over-the-Counter |
| OTF | Organised Trading Facilities |
| SEPA | Single Euro Payments Area |
| SFD | Settlement Finality Directive |
| SIPS | Systemically Important Payment Systems |
| UCITS | Undertakings for the Collective Investment in Transferable Securities |
| ZKP | Zero knowledge proof |