Digital finance: key priorities for the incoming Commission

1. Trends and opportunities from the use of technology in the financial sector

An industry representative noted that the use of technology in finance is driven by the objectives of increasing profitability and better meeting consumer demands, including working towards more financial inclusiveness. Focus to date in the market has primarily been on profitability and cost savings, a trend which has been amplified recently by inflation and macro-economic challenges. As a consequence, there has been less emphasis on customer-related evolutions. However, over the last 20 years, insurers for example have being using technology to improve their algorithms and customer data analysis to optimise pricing accuracy and risk mitigation. Progress on reducing exclusion and enhancing the personalisation of insurance products has been more limited. Policy measures might be needed to foster initiatives on financial inclusion.

A second industry representative agreed that digitalisation can enhance customer experience, accessibility and product innovation, as well as foster efficiency, profitability and risk management in the financial sector. Technology also supports new models of collaboration and new ways of providing financial services to clients, such as Banking as a Service (BaaS), which enables the provision of banking products to non bank third parties or platforms through APIs. Technology also leads to a more competitive landscape, which may be profitable for all market stakeholders provided there is a level playing field. The industry representative considered that financial exclusion is not a pressing issue for banking services in most developed European countries, where the number of unbanked citizens is limited. The Chair noted that, although there are few unbanked people in these countries, there is a risk of digital exclusion if people find it difficult to use banking apps.

A regulator highlighted that tokenisation, the digital representation of financial or real assets on distributed ledger technology (DLT), could be a major trend in the market in the coming years. Tokenisation offers significant potential advantages in terms of efficiency, transparency and accessibility for investors, allowing, for example, fractionalised ownership of real assets. However, the uptake of DLT has not been as fast as initially expected. This is partly because it is still an emerging technology with scalability issues remaining to be tackled. In addition, issues around operational resilience and how the governance framework may work in decentralised environments remain to be clarified. It is hoped that the European DLT pilot regime, which came into force in March 2023 and aims to encourage the uptake of DLT for securities trading and settlement by both established and new players, will support a further uptake of DLT in the securities market, together with the implementation of the Digital Operational Resilience Act (DORA).

A second regulator noted that in the insurance industry, technology is mainly used to enhance the processing of data. This is logical since insurance involves a great deal of data analysis, notably for pricing based on claim data. Most new developments in this area relate to artificial intelligence (AI) and data analytics. A recent EIOPA survey revealed that 61% of insurers are using AI daily. AI is still primarily being used for efficiency in the back office and to support claims management on the basis of photos, but is moving towards front office applications as well, such as price setting and risk assessments

The survey showed that digitalisation is still limited in other areas. Online sales are very low in the EU insurance sector, although this differs by market and is expected to change in the coming years. There are also limited open insurance developments in some markets in Europe. There is not a great deal of activity around blockchain or DLT in the insurance sector, although there could be applications in the area of parametric insurance for example, which involves automatic payouts triggered by pre-determined events. A move of big techs into the insurance market was anticipated by policy-makers, but has not yet happened. Insurance for damages related to crypto is another emerging area, although crypto is not yet used that much.

2. Challenges and risks associated with digitalisation

2.1 Customer protection and interconnectedness risks

A regulator stated that, while digitalisation is expected to play a critical role for the greater engagement of consumers in the capital market, this may give rise to new risks, for example related to increased cross-border offerings of investment products supported by digital channels, gamification, the role of influencers and social media, AI and crypto. ESMA has recently launched a survey of retail investors to assess how digitalisation is changing the relationship between financial market actors and consumers and how retail investor experience has changed with digitalisation in recent years. The outcome of this will feed into the thinking about future legislative developments.

The Chair observed that, although younger people are comfortable with digital channels and very digitally engaged with social media, they are possibly at a greater risk than older populations because they may be more

exposed to finfluencers and are used to scrolling quickly through information. Therefore they may not fully evaluate the risks of products to which they are exposed.

An official outlined several risks posed by digitalisation. First is the difficulty of keeping pace with the constant changes brought about by technology. Ensuring customer protection requires constant evolution in terms of skills and mindset on the side of financial intermediaries, supervisors and customers. Secondly, digitalisation generates a huge amount of capturable data, which increases security and privacy risks for consumers and operational resilience risks for financial firms. Thirdly, the increased interoperability of IT systems as a result of digitalisation increases the interconnectedness of different actors in the financial market, creating potential systemic and spillover risks. Finally, digitalisation also increases cross-sectoral risks, such as digital fraud.

2.2 Cyber and digital operational resilience risks

An industry representative emphasised the importance of addressing cyber risk and digital operational resilience risks. Many reports, for example from the World Economic Forum, the Bank of England and the Single Supervisory Mechanism, have highlighted cyber-risk as a critical global risk. To address the ever-evolving cyber threat landscape, the very best technology is needed. Cloud services can enhance the safety of financial infrastructure and services while supporting innovation, with access to greater analytical capability and computing power.

An industry representative noted that cyber-risk is being addressed by the implementation of the new Digital Operational Resilience Act (DORA) regulation. A regulator added that there is currently a gap in terms of insurance against cyber-risks which needs addressing also. The Chair noted that it is also important to raise awareness among financial services users about the various risks in the digital space including cyber-risks and the risks from phishing or spams.

3. Regulatory priorities for the next European political cycle related to digitalisation

3.1 Focus on the implementation of existing regulation

The Chair noted that a number of new legislations that may support further digitalisation and the mitigation of related risks have been adopted under the current legislature. These include the DLT pilot regime, the Payment Services Directive 3 (PSD3), the DORA framework, the Markets in Crypto-Assets Regulation (MiCA), as well as horizontal frameworks such as the AI Act and the EU strategy for data. These policies require adequate implementation and there is also the question of whether further policy intervention is needed.

An official stated that the priority is to properly implement the legislation that has already been adopted and to monitor its effects, before identifying the need for any additional or new rules. Digitalisation can have many positive impacts, but in order to harness them effectively it is important to also mitigate the challenges and risks that stem from it. How the financial sector is coping with the changes brought by digitalisation in its internal processes and in customer interaction and with the regulatory requirements aiming to ensure resiliency needs to be closely monitored. In some cases, existing regulations can be amended or their scope can be extended to increase their effectiveness. For example, extending the scope of the well-functioning anti-money laundering (AML) regime to unauthorised payment transactions would reduce the harmful effect of online fraud, allowing a suspension of these transactions and a gain of time to investigate the transactions.

A regulator agreed that continuous market monitoring is needed in this fast-developing area to identify possible gaps and determine whether they require additional legislation or amendments to existing rules. This monitoring is conducted at EU level in the joint committee of the ESAs together with the national competent authorities (NCAs) and cooperation is also needed at the international level to ensure sufficient regulatory convergence. There are individual dialogues for example with the UK and with the US regarding work on AI and DORA like projects.

Another regulator emphasised that much of ESMA's focus is now on implementing the rules that have been adopted, which need to be applied in practice in a timely manner. Establishing the regulatory technical standards for these new regulations is quite a challenging task. For example, MiCA will require significant policy implementation work with more than 30 mandates for ESMA.

An industry representative agreed that the focus in the next European political cycle should be on implementation and not on proposing new regulation. A large number of regulations have been adopted but have not yet been implemented, with many mandates and delegated acts to draft and implement. Interlinkages between the different digital regulations should also be carefully considered in this implementation work, for example between DORA and the Financial Data Access regulation (FiDA). There should also be consideration of interactions between regulation and private initiatives, such as between the digital euro and the European Payments Initiative (EPI). A consolidated view of the whole set of regulation is needed as well as a collective understanding of its implications for market stakeholders and of the possible challenges that need tackling.

3.2 New areas to address from a policy perspective

A regulator noted that two legislative proposals that are relevant for the digitalisation of financial services – FiDA and the Retail Investment Strategy (RIS) - are still being reviewed by the co-legislators. FiDA which aims to facilitate the sharing of personal and non-personal customer data held by financial sector intermediaries with third-party providers has many potential applications in terms of new online services and the RIS addresses social media engagement and finfluencers. Beyond the finalisation of these proposals, further

guidance may also be needed in areas such as the AI Act to better take into account the specificities of financial services. Concerning crypto-assets, more work will be needed on how to address decentralised finance (DeFi), depending on how it will develop in future. The possible need for a proper transaction reporting regime in MiCA should also be considered.

Another regulator agreed that DeFi should be further assessed to determine whether and how it may need to be addressed by legislation. Concerning AI, horizontal legislation makes sense, because there is no reason to treat technology differently per sector, but it may have different implications for different sectors. Guidance for the application of the AI Act to financial services will be drafted in 2024. As financial services are already heavily regulated, the implementation of the AI Act could lead to overlaps or gaps, both of which must be avoided. For this reason, it is very helpful that the AI Act incorporates the provision that the current sectoral supervisor will continue to supervise the requirements in the AI Act. Further clarification may also be needed in some areas of FiDA. The safe sharing of consumer data can lead to the improvement of online services and products and to more efficiency, but clarity is needed notably around whether the data to be shared concerns just raw data or potentially also intellectual property in rich data.

The Chair commented that the precise implications of the AI Act for the financial sector will need to be assessed over time, given the likely increase of AI use in the coming years. Concerning FiDA, an industry representative added that the practical modalities for implementing the financial data sharing schemes that are foreseen in FiDA also need careful consideration.

3.3 Key areas of focus for the implementation of adopted digital regulations

Some areas of focus for the upcoming implementation work on adopted digital regulations were suggested by the panellists.

A regulator suggested that the focus concerning the AI Act will be on the quality of the data and ensuring the fairness of processes using AI. For example, if AI is used to set the price of an insurance, the price should be set considering the customer's risk, not the likelihood of the person cancelling the policy if the price is increased. The process should also be inclusive, which means that it should be simple and understandable. This is already detailed in the principles for ethical use of AI that were drafted with industry and will be incorporated in the AI Act requirements.

An industry representative noted that in relation to the implementation of DORA, an important issue that needs considering is the highly sensitive nature of cyber-security information and of the information that technology providers such as cloud service providers (CSPs) handle. How supervisors and regulators will deal with this information is critical. This information is not just financial data but can also relate to national security or can be of systemic importance to the financial sector. In 2025, critical third-party providers (CTPPs), most likely including major CSPs, will need to start adapting to the DORA framework. CTPPs will need to consider how the risk management framework adapts to their activities.

4. The need to adapt policy-making and supervision to the digital world

4.1 Key principles needed for driving policy-making in the digital world going forward

An industry representative commented that regulation should follow four principles to support the digitalisation of the financial sector. First, EU competitiveness should be preserved. It is hoped that digitalisation challenges will be a significant part of Mario Draghi's upcoming report on the competitiveness of the European Union. Second, the safety of customers should be preserved. Third, the stability of the financial sector should be ensured. Fourth, the successful business models already in place should not be threatened by an unlevel playing field or irrelevant requirements.

Another industry representative agreed that strengthening the competitiveness of Europe vis-à-vis other regions such as the US should be a key policy objective in the next political cycle. This would involve facilitating investments in start-ups and ensuring that existing business models that work can be sustained. New regulations and supervision should contribute to an evolution of the financial industry, rather than a revolution. Some financial firms are concerned that FiDA might lead to a revolution if data sharing becomes mandatory, but this is unlikely. It is more likely that FiDA will aim to increase consumer outcomes in an evolutionary way.

The industry representative added that while protecting consumers from these new market development is an important objective with frameworks such as the AI Act or the Digital Markets Act which addresses gatekeepers, these 'reactive' approaches need to be combined with more pro-active regulations that aim to remove barriers to innovation, such as FiDA. Data is the key asset driving innovation in the European financial market. It is crucial that consumers own their own data and are free to share it to obtain improved service. Timing is a further aspect to consider. There should be caution around reacting to innovative changes in the market too early because regulating a new technology too quickly often may limit innovation and utilisation. Regulation must not be too slow either, as this would lead to negative impacts for consumers or other stakeholders. The right balance needs to be struck in terms of timing and also proactivity in order for Europe to lead the way in terms of digitalisation. If regulation is not proactive enough, other states will have a faster pace of digitalisation. The financial industry should be allowed to evolve and innovate, while ensuring that appropriate guardrails around consumer protection are in place.

A regulator emphasised that policy actions must remain customer-centric. An appropriate balance must be found between competitiveness and objectives such as providing consumer protection and access to finance. Competitiveness may also mean that some business models might not be sustainable.

4.2 Adapting supervisory and regulatory approaches to the digital world

An industry representative stated that supervision and financial regulation must also evolve with digitalisation and the authorities need to think 'outside the analogue box'. Regulatory frameworks and supervisory practices must be adapted to the new digitalised world. For example, operational resilience in a digital world is cross-sectoral and does not recognise geographical borders. Coordination at the international level is essential to ensure cyber resilience, as well as a collective effort from technology providers, the regulatory community and financial entities. DORA also requires that supervisors deal with information beyond the financial sector. In addition, there are a great deal of opportunities for the regulatory community to use technology for their own activities. Live surveillance of markets is already being used in the US. Upskilling will be critical and collaboration between technology providers and the regulatory community is crucial in this perspective.. The Digital Finance Academy is a very successful endeavour for example.

A regulator emphasized that cooperation at different levels among supervisors is essential to address digitalisation. Coordination between the European supervisory authorities (ESAs) and the NCAs is necessary for the implementation of MiCA, as the NCAs will be in charge of day to day supervision. A broader cooperation with authorities beyond the financial sector will be necessary to enforce AML requirements or ensure digital operational resilience and cyber-resilience in the context of DORA. Cooperation is also needed at the international level to address AML and cyber-risks and tackle the risks posed by financial players that operate on a global scale.

The regulator added that the implementation of certain rules will be challenging, particularly in areas where supervisors and industry players have limited experience, such as MiCA. In addition, effective consumer protection requires using the different levers available including regulatory standards and effective supervision and enforcement, which is a current area of focus for ESMA and the NCAs. Any potential for regulatory arbitrage must also be eliminated, which will require a common European regime for MiCA that addresses authorisation, supervision and enforcement in a common way.

Another regulator noted that supervisors will need to be trained and have a dialogue with innovative fintechs in order to fully understand the implications of new digital evolutions and have a sufficient level of comfort when considering these innovations. Some new developments can be confusing at first, but once they are better understood they can, in many cases, be related to existing activities and processes that they are attempting to improve. The Digital Finance Academy which was set up by DG Reform and the three ESAs for delivering training courses focusing mainly on the use of AI, is a good example of cooperation. An industry representative agreed that there is much value in training supervisors on new activities in a collaborative mode.

An official emphasised that digital risks, such as digital fraud and cyber-risks, are cross sectoral and require a cross-sectoral solution. Cooperation is needed between members of the financial intermediary system, supervisors, authorities, the IT sector, fintech and social media firms.

Conclusion

The Chair summarised that the panel had many common views. Business and consumer behaviour is changing because of digitalisation. A great deal of work has been carried out, but many of the rules still need to be implemented. The interaction between the different frameworks must be considered. A balance between giving space for innovation and making sure that consumers and investors are protected must also be sought.