TECH COMPANIES IN FINANCE: OPPORTUNITIES, CHALLENGES AND POLICY OPTIONS

Note written by Marc Truchet, EUROFI

1. Opportunities associated with the increasing presence of tech companies in the financial sector

Technology is playing an increasing role in the financial sector and becoming a key success factor in all the main sectors of finance and in all steps of the financial value chain, a trend which has accelerated with the pandemic. In this context, tech companies are intensifying their activities in the financial sector both directly, as providers of financial services and indirectly, as suppliers of ICT (information and communications technology) services for financial institutions.

Some bigtech firms have now acquired a significant market share in payment services in several jurisdictions including the EU and have also expanded in other sectors of finance such as credit underwriting, banking, insurance or asset management notably in Asia. Fintechs, which operate on a smaller scale, tend to focus on certain market segments where they provide innovative or targeted services (e.g. credit underwriting for SMEs, mobile payments, account aggregation, robo-advice, targeted digital banks...). These developments contribute to enhancing innovation and choice in the financial sector with new value propositions leveraging data analytics and alternative data in particular and they may also help to facilitate access to financial services for certain customer segments, with more customised and cheaper offerings.

Tech companies are also important providers of ICT services and infrastructure for the financial sector, leveraging their strong technology capabilities. The use of cloud computing in particular, which is mainly provided by subsidiaries of large bigtech companies at present, is rapidly expanding in the financial sector. First implemented for cost and flexibility reasons, cloud services are increasingly used to facilitate and optimize the use of sophisticated data analytics and also of artificial intelligence (AI), machine learning (ML) and distributed ledger technology (DLT) applications. Developing partnerships with tech companies such as cloud service providers (CSPs) is indeed a way for financial institutions to accelerate their digitalisation and implement more effectively data-driven processes and services, which may otherwise be hindered by their existing legacy systems. Some banks for example have concluded large-scale partnerships with CSPs in this perspective. On a smaller scale, financial institutions also partner with or purchase stakes in fintechs for the provision of new products and services or for improving their processes.

These partnerships enhance the ability of traditional financial institutions to innovate, differentiate themselves with new service offerings (e.g. with a higher degree of personalisation or pay per use models) and target new or specific customer segments, thus contributing to improve customer service and facilitating access to financial services and information for customers. Technology also helps financial institutions to implement more efficient and flexible operating models, allowing them to reduce their cost structure and improve their profitability and also to provide customers with better value for money. With technology, financial institutions can also upgrade their management and decision-making processes. Finally they can also enhance their security and operational resilience capabilities thanks to the security at scale and redundant architecture provided by cloud services and also with the use of new tools to fight cyber-risk and money laundering.

2. New challenges created by the developing role of tech companies in finance

The developing role of tech companies in finance however raises new questions in terms of financial stability, competition and supervisory capabilities, in addition to the challenges generally associated with the increasing digitalisation of financial services (e.g. greater exposure to potential cyber- and ICT operational risks, data protection and privacy issues...).

2.1 Financial stability issues

According to assessments of the BIS Financial Stability Institute[1], new vulnerabilities could be created by operational incidents affecting the activities of tech companies operating in the financial sector and particularly the larger ones, either directly or by spill-over effects across the different activities that they perform[2] and leading to possible systemic disruptions of financial services.

Such operational failures could have financial stability implications in cases where tech companies have acquired a significant position in the provision of certain financial services, which could be facilitated in the future by the capacity of large tech companies to rapidly scale up their operations in different data-driven

1. Big techs in finance : regulatory approaches and policy options – FSI brief – March 2021 and Fintech regulation: how to achieve a level playing field – Occasional paper N°17 – February 2021.

2. i.e. an operational incident in a specific business line that may impact the continuation of the activities conducted by the tech firm in the financial sector.

sectors such as finance, by leveraging their data analytics capabilities and wide user base and thanks to strong network effects[3].

Financial stability risks may also spread through the growing interconnections between tech companies and the financial sector. The outsourcing by financial institutions of core activities to tech companies, such as CSPs, indeed potentially exposes them to operational resilience[4] and business continuity risks caused by operational incidents affecting these tech providers, which may in turn threaten the continuous and adequate performance of critical financial activities. Another issue cited that however seems more remote are reputational risks, if a tech firm having partnered with a financial firm for the development and distribution of new products and services is accused of misconduct such as a breach of AML/CFT (anti-money laundering and combatting the financing of terrorism) rules or a violation of consumer protection obligations.

2.2 Competition and level playing field issues

Tech companies operating in the financial sector (fintechs or financial entities of bigtechs) also represent an additional source of competition for financial institutions, potentially creating new level playing issues.

Tech companies are subject to the same activity-based regulations as financial institutions, for the financial services that they provide. They need to obtain the relevant licence corresponding to these financial services and implement the same sectoral regulations as financial institutions. They are also subject to the same general regulations concerning data and consumer protection, AML/CFT, cyber-security, competition etc. as financial institutions, and will also be in the scope of the future digital finance regulations being negotiated in the EU as part of the Digital Finance Package[5].

However, despite this, there may be differences in the obligations that apply to different providers of similar financial activities, depending on whether they belong or not to a financial group subject to prudential regulation.

According to observations of the BIS Financial Stability Institute (FSI), the subsidiaries of regulated financial institutions providing similar services to tech entities, may be exposed to more stringent rules because they are part of a financial group subject to prudential regulation. Indeed banks, unlike non-banks such as tech companies[6], are regulated and supervised in a consolidated way, which means that their prudential requirements are calculated on a consolidated level[7] and impact all their subsidiaries (including those competing with tech providers such as those providing payment services). Bank deposits are also subject to contributions to a deposit protection scheme, which is not the case for e-wallets for example provided by some tech companies fulfilling a relatively similar function[8]. Banking subsidiaries are also usually subject to more stringent compliance and supervisory requirements, as part of a regulated financial group[9]. These level playing field questions are common to all non-banks providing financial services, however, they may be more acute in the case of some tech companies that have the capacity to scale-up more quickly than traditional non-banks by leveraging technology and data insights across their different activities, while also being exposed to potential spill-over effects from operational incidents across a broad range of activities.

Moreover, some rules designed to encourage innovation and digitalisation, such as open-banking rules may create differences in terms of data access between incumbents and new entrants. The example of the payment services directive (PSD2) is often emphasized by bank representatives. Under PSD2, banks have to give access to bank accounts for payment services provided by new payment providers (including tech companies), but they consider that there is an asymmetry in terms of data access. Indeed, while tech companies (as any payment service provider) are required to share the payment account

3. This is what the BIS describes as the DNA loop (Data analytics, Network externalities and interwoven Activities), which characterizes the activities of bigtechs - i.e. their capacity to leverage data analytics and the information gathered from a large user base for different activities in an effective way with significant network effects, together with their possible gatekeeper role. (BIS , Annual Economic Report 2019). Once a bigtech has attracted a sufficient mass of users on both sides of its platform, network effects kick in, accelerating its growth and increasing returns to scale: more data generated by users, in turn provide a better basis for data analytics, which enhances existing services and thereby attracts more users. Bigtechs also have a large and captive user base at their disposal, according to the BIS that allows them to scale up quickly in market segments that are outside their core business and are able to leverage state-of-the-art technology and also use insights derived from data analytics as a basis for developing novel services in other sectors.

4. The concept of operational resilience includes all factors affecting the ability of entities to deliver critical operations including outsourcing, business continuity, cyber-security.

5. The EU Digital Finance Package proposed by the Commission in September 2020 and that is currently being negotiated includes several legislations for supporting the digitalisation of the EU financial sector, adapting existing financial legislations to new developments such as crypto-assets, the use of AI and cloud services for financial services and also addressing the risks that digitalisation may pose for the financial sector. The package includes the Digital Finance Strategy, the Digital Operational Resilience Act (DORA), the regulation on Markets in Crypto-Assets (MiCA), the new retail payments strategy and the DLT pilot regime (see detail of the objectives of these different initiatives in the Eurofi Regulatory Update April 2021 'Digital Finance Strategy and Digital Finance Package: objectives and main proposals' https://www.eurofi.net/wp-content/uploads/2021/04/regulatory-update_lisbon_april-2021.pdf.)

6. Tech companies do not generally hold bank licences at present in the EU and US.

7. i.e. capital requirements are based on an assessment of the risks posed by the institution as a whole e.g. credit, market and operational risks.

8. Source Eurofi April 2021 Seminar summary "Is the current EU financial regulatory and supervisory framework fit for the digital age?".

9. There may be differences in the way the implementation of similar requirements is supervised, because of differences in the way supervision is conducted across sectors. According to the BIS FSI, supervisors may apply more stringent standards (e.g. concerning consumer protection, AML/CFT or data protection) to credit institutions than to fintech players for example, because of proportionality principles and also due to the fragmentation of supervision (except when supervision is organized according to a twin-peaks functional model).

information of their clients, upon their consent, with other licensed third-parties that provide payment initiation and account information services, they are not required to share any other data generated on their platforms, which means that banks cannot access the full extent of the data generated by these new players concerning their clients. This creates a potential competitive disadvantage for financial institutions in their view, in a context where access to relevant customer data is increasingly constituting a source of innovation and differentiation, and could restrict the future provision of digital financial services leveraging a wide range of customer data. GDPR rules can potentially support a wider portability and sharing of data in this context, since they establish the principle of user data ownership, requiring firms to share clients' data with third parties at the customers' request and create structures for European data protection authorities to cooperate. However GDPR is limited by the fact that it applies only to the data of natural persons (and not to non-financial company data for example) and does not contain a technical standard for the transmission of information that would guarantee its efficient use by the recipient.

A further issue that has been cited is the difficulty to address, with current competition policy, which is mostly ex-post, potential competitive distortions[10] that may be caused by rapidly scaling-up tech business models or services. Some policy-makers argue that ex-ante entity-specific rules would be needed to address certain potential anti-competitive practices of large tech companies acting as so-called gatekeepers. This is the direction taken for example with the measures recently proposed by the Commission in the EU Digital Markets Act (DMA), which aim at preventing gatekeepers from imposing unfair conditions on businesses and consumers and at ensuring the openness of digital services[11].

2.3 Supervisory challenges

The increasing role of tech players in the financial sector and the use of technologies, which are outside the scope of those used traditionally in the financial sector also create challenges for regulators and supervisors in terms of skills, resources and working processes. Fast changing technologies can also create new regulatory loopholes if financial regulations do not evolve fast enough with the latest digital innovations.

Providing appropriate guidance regarding these evolutions, i.e. with a balance between risk mitigation and innovation objectives, indeed requires a detailed understanding of the opportunities and risks associated with new technologies for different financial activities and of their interaction with existing financial and operational risks.

Financial supervisors are also faced with the additional complexity of monitoring a wider range of market participants and operating models (with an increasing role of third-party ICT service providers of different natures for example). The speed of change and innovation happening in the tech sector both in terms of technology and operating model, combined with on-going innovation in the financial sector, is a further challenge.

3. Policy options for addressing the challenges associated with the development of tech firms in finance

3.1 Adapting the financial regulatory and supervisory framework to the digital age

A first option to address potential opportunities and risks associated with the growing role of tech companies in finance is to ensure that the regulatory and supervisory approach is adapted to this transformation. The EU financial policy framework has not evolved significantly so far with the advent of digitalisation in finance[12], with the exception of payments in particular (with PSD 2). In addition, most EU policy frameworks concerning digitalisation and technology have remained horizontal, applying to all sectors[13].

The situation is however due to change in the EU with the upcoming implementation of the Digital Finance Package proposed by the Commission in September 2020. This legislative package includes a Digital Finance Strategy - which aims to adapt the financial regulatory and supervisory framework

10. e.g. potential issues related to the bundling of different services, personal data misuse or discriminatory access conditions for participants.

11. Gatekeepers are defined by the European Commission as companies that meet the following criteria: they have a strong economic position, significant impact on the internal market and are active in multiple EU countries; have a strong intermediation position, meaning that they link a large user base to a large number of businesses; have (or are about to have) an entrenched and durable position in the market, meaning that it is stable over time. The DMA for example proposes that gatekeepers should not treat services and products offered by the gatekeeper itself more favourably in ranking than similar services or products offered by third parties on the gatekeeper's platform; prevent consumers from linking up to businesses outside their platforms; prevent users from un-installing any pre-installed software or app if they wish to.

12. The situation is similar at the international level. Some sectoral regulations have been updated in areas with significant fintech penetration, such as wealth management, payment services or insurance and efforts have been made to update existing regulations to eliminate barriers to digitalisation but rules have not been extensively modified. New players therefore compete with incumbent companies using rules that existed before they emerged. The creation of new regulatory categories, such as digital banks, is more an exception than the rule. Clearer and more determined policy action can be seen for cryptocurrencies however. For example anti-money laundering and combatting the financing of terrorism (AML/CFT) rules have been adjusted by international standard setters, notably the Financial Action Task Force (FATF), the global AML / CFT watchdog, to incorporate crypto-asset service providers. See Eurofi April 2021 Seminar Summary "Is the current Eu financial regulatory and supervisory framework fit for the digital age?"8. Source Eurofi April 2021 Seminar summary "Is the current EU financial regulatory and supervisory framework fit for the digital age?".

13. A fintech action plan on how to harness the opportunities presented by technology-enabled innovation in financial services was published by the Commission in 2018, but it focuses mainly on measures to explore the potential of fintech and the exchange of best practices, rather than on regulatory changes.

to the increasing digitalisation of the EU financial sector, remove potential obstacles to digitalisation and also address possible new risks and level playing field issues related to this digital transformation – as well as several other legislative proposals targeting different areas of digitalisation: the Digital Operational Resilience Act (DORA), the regulation on Markets in Crypto-Assets (MiCA), the new retail payments strategy and the DLT pilot regime.

Efforts are also being made to adapt regulatory and supervisory approaches to digital innovation. New concepts such as innovation hubs or sandboxes have been put in place by many national competent authorities over the last few years in order to monitor fintech developments, facilitate the safe testing of new fintech concepts and accelerate the learning curve of regulators in this area. Specific policy regimes, such as the one proposed in the EU DLT pilot regime, also aim to allow market players and regulators to gain more experience with the use of DLT technology in securities markets, while ensuring an appropriate monitoring of risks.

3.2 Optimizing the mix of activity- vs entity-based regulation

The appropriate mix of activity- and entity-based regulation for supporting the development of tech companies in finance and tackling related challenges is also being considered. Many market stakeholders advocate the use of 'same activity, same regulation' principles for guiding financial services policy in order to ensure a level playing field between financial and non-financial players such as tech companies and also an equivalent mitigation of risks. This would potentially imply a wider use of activity-based regulations, applying the same system of rules to all types of entities providing the same activity.

The FSI however points out that while an activity-based regulatory approach can help to eliminate regulatory arbitrage in the provision of a given activity and is also effective for tackling the risks related to the operation of this activity (consumer protection, conduct, AML / CFT risks for example), it is insufficient for mitigating risks that may stem from the combination of different activities within a given entity, such as financial stability and competition risks. Another caveat of activity-based regulation is that activities must be defined precisely, which can be challenging with rapidly changing and hard to define fintech activities. For these reasons, most regulatory frameworks in the financial sector contain both activity- and entity-based rules.

For example in the banking sector, maturity transformation, which involves a combination of deposit taking, investment and underwriting activities, is a major potential source of financial stability risk, alongside liquidity transformation risk[14]. In order to tackle these risks, prudential capital requirements are imposed on banks at a consolidated level - i.e. at the bank entity-level - in addition to activity-based requirements, with the result that a different set of obligations may be imposed on a given activity, depending on the characteristics of the entity performing it (e.g. a deposit-taking bank or a non-bank), as mentioned previously in § 2.2. Banking regulators justify this approach by the fact that the same credit underwriting activity for instance, may generate different risks for the financial system, depending on how the activity is funded[15] (e.g. by the own resources of the firm providing the activity, market leverage or deposits taken from the public). The maturity transformation business of banks therefore requires a specific prudential regulatory treatment for their credit provision activities, which may not be necessary for non-bank credit providers that cannot accept deposits.

Tech companies do not perform such risk transformation activities at present in the EU and therefore do not require the same kind of prudential requirements. However, in the view of the FSI, they may be associated with other risks that can threaten the adequate functioning of the financial system, as previously mentioned, such as operational resilience and fair competition risks, which would not be appropriately addressed from a policy perspective if the focus is exclusively on specific financial activities. The FSI has therefore suggested that a combination of activity-based and entity-based regulation should be considered for addressing the different risks posed by tech companies operating in the financial sector.

The proposed EU Digital Markets Act (DMA) and Digital Operational Resilience Act (DORA) both adopt this type of approach, since they include specific entity-level measures for tech companies playing a significant role in the market, together with activity-based rules. As per the Commission's DORA proposal, a specific regime would be introduced for third-party ICT providers considered to be 'critical' for the functioning of the financial sector[16], subjecting them to an EU oversight framework in order to improve the management of the risks posed by these providers. At the global level, the FSB is also working on the regulatory and supervisory issues relating to outsourcing and third-party relationships, addressing both activity-related and entity-related risks and issues: i.e. potential stability risks to financial institutions associated with third-party providers becoming single points of failure, because of their criticality and lack of substitutability, and also supervisory approaches for managing outsourcing and third-party risks[17].

14. Source Eurofi April 2021 Seminar Summary.

15. Source BIS FSI Speech F. Restoy 16 June 2021.

16. Based on criteria such as the systemic impact of a potential failure of the provider, the systemic character of financial entities that rely on the service provider and its geographical coverage and degree of substitutability.

17. Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships - Discussion paper – FSB – November 2020.

This combined approach would also imply an entity-level supervision for monitoring the build-up of risks from tech firms and the evolution of their business models, potentially requiring a close cooperation between financial regulators and other sectoral, competition and data protection authorities, as well as supervisory cooperation at the international level, since many large tech companies have their headquarters outside the EU[18].

18. The challenges of implementing a wider-scale supervision of tech companies have been stressed by T. Adrian (IMF) for example in a recent paper (Bigtechs in financial services, June 16 2021). Many of the larger tech companies are based outside of Europe at present, therefore potentially requiring a cooperation between EU supervisors acting as host supervisors and US or Chinese supervisors acting as home supervisors and in charge of supervising possible entity-based requirements at group level.