EACB Comments

Implications of fintech developments for banks and bank supervisors - consultative document

Brussels, 31st October 2017

Contact:

For further information or questions on this paper, please contact:
- Mr. Volker Heegemann, Head of Department (v.heegemann@eacb.coop)
- Mr. Marco Mancino, Deputy head of Department, Banking Regulation (m.mancino@eacb.coop)

General comments

The members of the EACB welcome the opportunity to comment on the BCBS consultative document on the implications of Fintech developments for banks and supervisors.

In general, EACB members appreciate the fact that the BCBS decided to align the definition of FinTech with the one given by the Financial Stability Board, as done also by the EBA in its discussion paper on the EBA's approach to financial technology (Fintech), i.e. "*Technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services*".

Indeed, the term Fintech is most of the time used synonymously with "Fintech start-up companies", thus ignoring that technology-enabled innovation in financial services does not depend on the size or legacy of a firm and that innovative financial technology–based solutions and services are increasingly being developed by banks.

In our view, it is particularly important to agree on a common understanding given that the definition can influence how supervisors approach Fintech.

Having said that, using the proposed definition risks putting bank driven developments such as instant payment outside the Fintech perimeter as it might not be considered as being based on a particular technology other than the increase in computer power and digitalisation of processes in general. The instant payments development however, does have an important impact on "*business models, applications, processes and products and has an associated material effect on financial markets and institutions and the provision of financial services*". It also could increase or reduce certain risks depending on its relation with other Fintech developments. This report having the objective to "*identify and assess risks and related supervisory challenges, both for banks and bank supervisors*", we therefore believe that instant payment should be given a place in this report either as part of the Fintech definition or as an innovation that needs to be seen in combination with Fintech developments.

More in general, the use of technologies by financial services firms is not new per se. Financial services firms have long implemented internal technological solutions to support the provision of services to their customers and to ensure that they comply with their regulatory obligations. As such, it should be considered that the essential nature of the banking business (i.e. risk and maturity transformation) is not put into question by the use of technological solutions.

What we would particularly like to stress is that a level playing field is key to assure not only fair competition but also a sound prudential environment and consumer protection.

The same regulatory conditions and supervision should apply to all actors who seek to innovate and compete on Fintech: large digital players (big tech firms), financial institutions players (incumbent banks) and Fintech start-ups players.

At the same time, the regulatory framework while keeping entry barriers to a minimum, should also not hinder incumbents' ability to innovate and develop. Due to entry of global internet giants/business platforms and new agile challenger firms using fintech, customer expectations have changed dramatically. Banks should be able and allowed to innovate a new breed of services to remain relevant. For example, some of our members are actively refining old banking products (such as mortgage and car loans) into combined packages, like smart housing and mobility-as-a-service concepts. These services include also non-financial elements and more active cooperation with third parties. We encourage regulators to adopt proactive approach to the evolution of future banking services.

The principle of "same services, same risks, same rules and same supervision" in order to ensure a high level of consumer protection and preserve financial stability should always apply. It would not make sense to have deeply revised the prudential framework and established recovery and resolution tools, if threats to financial stability are allowed only for the sake of technological novelty. In this regard, the European Central Bank has for instance launched a first consultation to assess the criteria for licensing FINTECH banks.

Specific comments

Observation 1: The nature and the scope of banking risks as traditionally understood may significantly change over time with the growing adoption of fintech, in the form of both new technologies and business models. While these changes may result in new risks, they can also open up new opportunities for consumers, banks, the banking system and bank supervisors.

Recommendation 1: Banks and bank supervisors should consider how they balance ensuring the safety and soundness of the banking system with minimising the risk of inadvertently inhibiting beneficial innovation in the financial sector. Such a balanced approach would promote the safety and soundness of banks, financial stability, consumer protection and compliance with applicable laws and regulations, including anti-money laundering and countering financing of terrorism (AML/CFT) regulations, without unnecessarily hampering beneficial innovations in financial services, including those aimed at financial inclusion.

We have doubts about the observation that the nature of banking risks will change so significantly in every respect, especially regarding solvency risk.

Nevertheless we would fully subscribe to the intentions of recommendation 1. We do also believe however, that the arrival of Fintech necessitates a more holistic view, in particular of supervisors, of the different influences on banks and their business models. Digitalisation and Fintech are but one development impacting those bank business models. Regulatory demands (both where it concerns product regulation, consumer protection and prudential regulation) and the consequences of competition policy are equally impactful.

Unfortunately the latter are not always consistent and sometimes even contradict each other. Examples in Europe are that of the Payment Services Directive which opens up accounts held by bank clients to payment initiation and data access by third parties without allowing banks the necessary control mechanisms to manage the resulting operational, and cyber risk. Additionally, we understand that competition authorities in some Member States prohibit banks from launching mobile payment applications because of their dominant position whereas the success of such application depends on the amount of banks (and bank clients) that support it. A balanced approach would have to originate from a holistic approach that takes into consideration the impact of product oriented regulatory tendencies, competition policy drivers, prudential legislation and supervisory objectives.

In more general terms we would like to point out that FinTech stand for new technology, but independent from the size of the company, i.e. whether it is implemented by an incumbent bank of a new start-up. In general, the principle "same business, same risk, same regulation" should be the overall principle guiding every regulation. A regulatory framework that creates room for regulatory arbitrage would trigger a "race to the bottom". The under-regulation of certain participants would create the weak spots of the entire system

As per the comments in our introduction, we believe that the concept of instant payments desires particular attention and cannot be left out of the scope of this report. It has consequences on "*business models, applications, processes and products and has an associated material effect on financial markets and institutions and the provision of financial services*", creates new risk but also create new opportunities.

Finally, the main change of digitalisation (and only to a certain degree by FinTech) is the emergence of global internet juggernauts from the West (Google, Facebook, Amazon) and East (Baidu, WeChat, Alibaba), Their business model of "monetizing customer date for advertisement" is a huge change to the industry in general and includes banks, but it cannot be confused with banking. Banks have to be aware of (i) regulatory arbitrage and (ii) global arbitrage, but so do regulators and supervisors. It should be avoided that while banks are extremely well regulated, the shadow banking sector is left free to accumulate risk.

In this context we would also like to refer to robo-advice, when this form of advice is given in the context of traditional banking business, it remains within the regulatory framework already in place for the protection of the customer. It should be avoided that online providers are placed at a competitive advantage in terms of less stringent requirements and that the duty of care is left only in the hands of the banks that will eventually provide the investment service.

Observation 2: For banks, the key risks associated with the emergence of fintech include strategic risk, operational risk, cyber-risk and compliance risk. These risks were identified for both incumbent banks and new fintech entrants into the financial industry.

Recommendation 2: Banks should ensure that they have effective governance structures and risk management processes in order to identify, manage and monitor risks associated with the use of enabling technologies and the emergence of new business models and entrants into the banking system brought about by fintech developments. These structures and processes should include:

- robust strategic and business planning processes that allow banks to adapt revenue and profitability
- plans in view of the potential impact of new technologies and market entrants;
- sound new product approval and change management processes to appropriately address changes not only in technology, but also in business processes;

- implementation of the Basel Committee's Principles for sound management of operational risk (PSMOR) with due consideration to fintech developments; and
- monitoring and reviewing of compliance with applicable regulatory requirements, including those related to consumer protection, data protection and AML/CFT when introducing new products, services or channels.

We agree with the risks identified in observation 2. However, and also in connection with Observation 1, it should not be forgotten that the banking business per definition entails the collection of deposits, risk transformation (solvency risk), maturity transformation, and scale transformation; none of these elements is affected by "FinTech" per se. Banking risk is not generated by technology as it stems from the generic function of banks to provide risk transfer. Changes in technology may rather affect strategic risk, operational risk (finance and data related), cyber-risk (finance and data related) and compliance risk.

Having said that, the technological developments that drive the Fintech phenomena should not only be a concern for banks and banking supervisors , but also for data protection authorities, those authorities monitoring cyber resilience of important public infrastructures.

An element that is rightly gaining growing emphasis at least for the ECB supervision is cybercrime and the IT disruptions. This is a multifaceted issue for which various aspects need consideration: e.g. more digitalisation, higher speed in execution of payment transactions as a result of instant payments, increased banking ecosystem and transaction chain increases the risk of incidents and attacks; the danger of attacks and disruptions to payment systems; the effects on trust when incidents occur; the open question on responsibility ownership for credit institutions when they do not control the entire process with the client any longer and when customer data are stored outside the direct control of the bank; new market participants and their offer in a changing labour market.

Fintechs start-ups are not better placed than banks to address these questions or are sometimes not even asked to address these questions. This should not be the case. Moreover, while stressing the importance of the processes and structures that have to be put in place both in banks and fintechs, we nevertheless fear that the severe breach of any such requirements by fintechs could leave consumers much less protected if the latter do not dispose of sufficient insurance or capital.

The European supervisors and regulators have been already stressing the questions of cyber and IT risk. For the ECB cyber risk is a supervisory priority. Also the EBA has been active on the topic as it issued draft Guidelines on the assessment of the Information and Communication Technology (ICT) risk in the context of the Supervisory Review and Evaluation Process (SREP). The draft guidelines will also help establish the necessary management focus and support for important risks such as the ever-growing cyber risks and important evolutions like FinTech that may have a pervasive impact on the institution's business model, competitiveness and profitability.

Turning now to the proposed recommendation we would like to note again the need to take a holistic view at the environment in which banks operate and not to look at the Fintech phenomena in isolation but to consider also the challenges that the regulatory environment presents. We would have the following observations:

- Rec 2.1: the EU several pieces of legislation exist that curtail banks' freedom to price their services or recover costs for services performed (MIFID2, PSD2, other pieces of payment/bank account legislation) which is not necessarily applicable to other actors. Looking ahead, the tendency is for product regulation to become more and more invasive thereby limiting banks freedom to adapt revenue and/or profitability.
- Rec 2.3: in the EU specific legislation exists (MIFID 2) addressing particular banking business lines that impose the implementation of very detailed product governance rules making different parts of the market dependent on each other (product manufacturers and product distributors) and thus limiting the flexibility and speed with which banks can individually adjust to technological or other developments.
- Rec 3.5: as a result of the increase in legislation that occurred in the last 5 years, banks have recruited an important number of additional compliance staff. Indeed compliance departments have grown exponentially. Part of the challenge for these departments is indeed, to balance all existing regulatory requirements with the need to innovate.

On a general level, the EACB would therefore agree with the recommendation made but it would call for an awareness both of banks and bank regulators of the need to take a holistic view in innovation that includes fintechs.

Observation 3: Banks, service providers and fintech firms are increasingly adopting and leveraging advanced technologies to deliver innovative financial products and services. These enabling technologies, such as artificial intelligence (AI)/machine learning (ML)/advanced data analytics, distributed ledger technology (DLT), cloud computing and application programming interfaces (APIs), present opportunities, but also pose their own inherent risks.

Recommendation 3: Banks should ensure they have effective IT and other risk management processes that address the risks of the new technologies and implement the effective control environments needed to properly support key innovations.

In the EU, banks will have to respect the measure that the different national supervisory authorities will develop based on the different sets of guidelines that are being/have been drafted already in this context by European supervisory authorities such as:

- the EBA guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)
- the forthcoming EBA guidelines on security measures for operational and security risks of payment services under PSD2, which take into consideration the EU Network and Information Systems (NIS) Directive34 5 6 , the BCBS principles on operational risk, the US NIST Framework, and the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures .

Observation 4: Banks are increasingly partnering with and/or outsourcing operational support for technology-based financial services to third-party service providers, including fintech firms, causing the delivery of financial services to become more modular and commoditised. While these partnerships can arise for a multitude of reasons, outsourcing typically occurs for reasons of cost-reduction, operational flexibility and/or increased security and operational resilience. While operations can be outsourced, the associated risks and liabilities for those operations and delivery of the financial services remain with the banks.

Recommendation 4: Banks should ensure they have appropriate processes for due diligence, risk management and ongoing monitoring of any operation outsourced to a third party, including fintech firms. Contracts should outline the responsibilities of each party, agreed service levels and audit rights. Banks should maintain controls for outsourced services to the same standard as the operations conducted within the bank itself.

In general, we see different reactions in the market to the Fintech phenomenon, across different kinds of banks (cooperative or non-cooperative) and across countries, varying from:

- banks developing their own technological solutions that mirror the strong points of Fintech challengers;
- banks partnering with Fintech challengers for technological support of their customer-bank relationship;
- banks buying Fintech challengers to incorporate their business models into their own.

However, the emergence of FinTech has to be seen as a development of technology with the normal risk of any evolution in technology.

This has to be distinguished from the current trend of global monopolies of so-called business platforms (Google, Facebook, Amazon and Baidu, WeChat, Alibaba etc.), which may have the potential to change global business models.

Outsourcing per se would not be treated as (additional) operational risk - see e.g. Jürgen Bott and Udo Milkau "Outsourcing Risk – a separate operational risk category?" in: Journal of Operational Risk Management, Vol. 10/3, 2017 – and an institution specific approach would be the most appropriate tool to assess any potential risk. In the same vein the outsourcing to fintechs should be treated on the basis of the same principles and guidelines as any other outsourcing.

Having said that, and coming back to the proposed recommendation, we would argue that the EU's Payment Services Directive – by bringing third parties into the payment transaction chain – forces banks to accept that the payment initiation leg of a payment transaction and the customer authentication for that transaction is sourced from outside the bank, with a risk of inconsistency on the understanding and treatment of outsourcing.

As the recommendation rightly proposes, where processes are sourced from parties outside the bank, "*contracts should outline the responsibilities of each party, agreed service levels and audit rights. Banks should maintain controls for outsourced services to the same standard as the operations conducted within the bank itself*". The said Payment Services Directive however, does not allow banks to impose such contracts. We believe that this constitutes an inconsistency between product legislation on the one hand and supervisory guidelines on the other and leaves banks exposed to an operational risk that is more difficult to manage.

Observation 5: Fintech developments are expected to raise issues that go beyond the scope of prudential supervision, as other public policy objectives may also be at stake, such as safeguarding data privacy, data and IT security, consumer protection, fostering competition and compliance with AML/CFT.

Recommendation 5: Bank supervisors should cooperate with other public authorities responsible for oversight of regulatory functions related to fintech, such as conduct authorities, data protection authorities, competition authorities and financial intelligence units, with the objective of, where appropriate, developing standards and regulatory oversight of the provision of banking services, whether or not the service is provided by a bank or fintech firms.

The EACB would support this recommendation, as it would lead to a more holistic view of the challenges that banks face, be it regulatory or Fintech related. Having said that, this cooperation also include authorities developing prudential and product regulation.

Observation 6: While many fintech firms and their products – in particular, businesses focused on lending and investing activities – are currently focused at the national or regional level, some fintech firms already operate in multiple jurisdictions, especially in the payments and cross-border remittance businesses. The potential for these firms to expand their cross-border operations is high, especially in the area of wholesale payments.

Recommendation 6: Given the current and potential global growth of fintech companies, international cooperation between supervisors is essential. Supervisors should coordinate supervisory activities for cross-border fintech operations, where appropriate.

The EACB would fully support this recommendation.

Observation 7: Fintech has the potential to change traditional banking business models, structures and operations. As the delivery of financial services becomes increasingly technology-driven, reassessment of current supervision models in response to these changes could help bank supervisors adapt to fintech- related developments and ensure continued effective oversight and supervision of the banking system.

Recommendation 7: Bank supervisors should assess their current staffing and training models to ensure that the knowledge, skills and tools of their staff remain relevant and effective in supervising new technologies and innovative business models. Supervisors should also consider whether additional specialised skills are needed to complement existing expertise.

The EACB would support this recommendation

Observation 8: The same technologies that offer efficiencies and opportunities for fintech firms and banks, such as AI/ML/advanced data analytics, DLT, cloud computing and APIs, may also improve supervisory efficiency and effectiveness.

Recommendation 8: Supervisors should consider investigating and exploring the potential of new technologies to improve their methods and processes. Information on policies and practices should be shared among supervisors.

Observation 9: Current bank regulatory, supervisory and licensing frameworks generally predate the technologies and new business models of fintech firms. This may create the risk of unintended regulatory gaps when new business models move critical banking activities outside regulated environments or, conversely, result in unintended barriers to entry for new business models and entrants.

Recommendation 9: Supervisors should review their current regulatory, supervisory and licensing frameworks in light of new and evolving risks arising from innovative products and business models. Within applicable statutory authorities and jurisdictions, supervisors should consider whether these frameworks are sufficiently proportionate and adaptive to appropriately balance ensuring safety and soundness and consumer protection expectations with mitigating the risk of inadvertently raising barriers to entry for new firms or new business models.

Indeed, supervisory and licensing frameworks predate adoption of current technologies and evolving business models. The legislation might also be outdated vis-à-vis new technologies (such as blockchain, cloud computing, etc.). This is huge challenge for regulators as there might be regulatory gaps or, on the other hand, inappropriate hindrances to adoption of new technologies. We suggest regulators and supervisors to adopt forward-looking and principles-based approach to interpretation of current rules. The focus should be on core regulatory principles aiming at stability and consumer protection rather than detailed interpretation of rules than could be outdated.

It is worth noting in this context that the European Central Bank has issued a consultation on this topic.

Observation 10: The common aim of jurisdictions is to strike the right balance between safeguarding financial stability and consumer protection while leaving room for innovation. Some agencies have put in place approaches to improve interaction with innovative financial players and to facilitate innovative technologies and business models in financial services (e.g. innovation hubs, accelerators, regulatory sandboxes and other forms of interaction) with distinct differences.

Recommendation 10: Supervisors should learn from each other’s approaches and practices, and consider whether it would be appropriate to implement similar approaches or practices.

The EACB is not against the mentioned initiatives but would consider that in this fast-changing environment, a level playing field is key to assure not only fair competition but also consumer protection. In addition, we believe that these initiatives should not become an element of competition between countries to attract Fintech and lead to a race to the bottom on the rules that have to be respected.

Regulatory sandboxes should provide an efficient gateway for both new entrants and incumbents in the FinTech sector, by providing not only advice in relation to regulatory requirements they will need to comply with, but also as a testing facility in the context of national specificities. Many European cooperative banks are investing significant amounts in new technology. Sandboxes or innovation hubs could provide platform for enhanced dialogue with regulators and supervised entities. It also helps regulators and supervisors to familiarise with new technologies.

It should however be stressed that sandboxes should not be lowering regulatory standards, as consumer protection is paramount. We support the recommendation made in the BCBS's survey that sandbox participants must inform consumers and all relevant stakeholders that the company is providing the service under a sandbox regime.

Even though we are not convinced that sandboxes can provide better results compared to market-driven innovation, any guideline should ensure sandboxes or other innovations hubs or similar regimes include both new (start-up) and incumbent (e.g. banks) FinTech providers and that a level playing field with those outside the sandbox is in place by ensuring transparency on the experiments going on and any regulatory 'lenience' considered.

Finally it has to be kept in mind that a sandbox is a security mechanism for separating entities to limit the effect of failures and especially to exclude system failures. However, once an entity or several entities reach a certain dimension and/or importance, such a "separation approach" comes to its limits.