European Commission's Public consultation on FinTech: a more competitive and innovative European financial sector

Joint answer from Banque de France and Autorité de contrôle prudentiel et de résolution (ACPR)

1. Fostering access to financial services for consumers and businesses

1.5 What consumer protection challenges / risks have you identified with regards to artificial intelligence and big data analytics (e.g. robot advice)? What measures, do you think, should be taken to address these risks / challenges?

- **Assess whether there is a need for a regulatory principles on governance and oversight of algorithms and data analytics that would complement the product approach of the current EU regulation.**

Banque de France and ACPR recognize the potential merits and benefits of artificial intelligence and big data analytics for consumers, notably to offer more tailored products and value-added financial advice to new ranges of consumers.

As identified by the ESAs Joint Committee working groups on Robo-advice and Big Data, artificial intelligence and big data analytics may also give rise to new and evolving risks:

- the increased information asymmetry between the consumer and the provider (especially when there is no access to human advice), when new data processing tools result in a "black box"
- the financial exclusion (through basic exclusion or prohibitive pricing) because innovative tools allow finer profiling of consumers and mitigate the principle risk pooling

However, it is fair to mention that those risks have not materialized yet partly because artificial intelligence and big data analytics are still nascent. Thus, as part of its consumer protection task, ACPR actively monitors new data processing tools through usual controls and pro-active dialogue with innovative financial players.

Based on that assessment, ACPR has come to the following conclusions:

- Proper enforcement of personal data protection regulation by all types of players addressing European consumers is very crucial, including by non-EU platforms. Better cooperation between financial supervisors and data protection authority is needed in that area. In France, the data protection authority (CNIL) is an active member of the Fintech Forum set up by the ACPR and the AMF that gathers public authorities and Fintech representatives about regulatory challenges.
- Current regulation provides appropriate concepts that should remain valid in a digital world. In particular, the obligation of consumer fair treatment that exists in most the

recent European directives in the field of financial services should be implemented in algorithms uses for selling financial products and/or providing advice. Consequently, there may be a case for developing a set of principles around the "*governance and oversight of algorithms and data analytics*" to ensure that those tools which substitutes to human procedures and/or human salesforces can also deliver fair outcomes to the customer, taking into account the client's best interest.

1.6 Are national regulatory regimes for crowdfunding in Europe impacting on the development of crowdfunding? In what way? What are the critical components of those regimes?

- **Yes. The French regulatory regime for crowdfunding has supported the development of crowdfunding in a safe way**

The French regulation promotes a proportionate approach for crowdfunding (direct matching of fund-seeker and fund-provider through a web-platform). This regime has been introduced in 2014 and subsequently revised in 2016 for adapting some rules after two years of concrete experience. According to publicly-available statistics, France counts around one hundred of crowdfunding platforms and is now the 2nd largest crowdfunding market in Europe.

In details, the French regulation has introduced two statuses for crowdfunding platforms: one for equity platforms that are supervised by the Autorité des Marchés Financiers (AMF), one for gift and lending platforms that are supervised by the ACPR with respect to consumer protection and AML-CFT obligations.

The regulatory regime for crowdlending platforms is proportionate to the scale of risks:

- Platforms must be registered with fit and proper requirements but there is no authorization process so that they can start their activity rapidly
- Platforms must contract liability insurance but there is no capital requirements because they never hold the credit risk on their balance sheet
- Platforms must publish adequate disclosures about the project to make the "crowd" aware of the risks associated with the lending activity. There are therefore transparency requirements regarding project selection, project assessment, default rates and annual reports but there is no advisory duty.
- Since there is no advisory duty, financing must be provided in the frame of a well-defined project. The amount that can be raised on a platform is also capped at EUR 1 million and the amount individuals can lend for a project is also capped at a low level (2000 euros).

1.7 How can the Commission support further development of Fintech solutions in the field of non-bank financing, i.e. peer-to-peer/marketplace lending, crowdfunding, invoice and supply chain finance?

- **A common and proportionate European regulatory framework for crowdlending may be envisioned once the market is more mature.**

Some French crowdlending platforms are expanding their activity to other EU countries to gain in volumes and to reach a profitable size. Some platforms that are registered or licensed in other countries are also seeking to expand their activity in France. Once the market is more mature, the Banque de France and the ACPR consider that there could be benefits to think about a common and proportionate European regulatory framework for crowdlending activity. It may further support this new source of funding for businesses and investment for individuals at a European scale (cross-border allocation of savings). In order to be consistent

with the CRD4/CRR framework and to avoid any kind of regulatory arbitrage, these platforms would not be allowed to make use of their balance sheet for carrying out this intermediation.

At the same time, the business model of crowdlending platforms is evolving rapidly. While the loans originated by strictly defined peer-to-peer lending platforms are directly purchased by retail investors, the business model of lending platforms are currently turning into marketplace lending platforms, where loans can be purchased or financed both by retail and institutional investors. It would be worth monitoring and comparing national developments in that area.

1.8 What minimum level of transparency should be imposed on fund-raisers and platforms? Are self-regulatory initiatives (as promoted by some industry associations and individual platforms) sufficient?

- **With regards to the positive crowdfunding experience in France, Banque de France and ACPR consider that public regulation can be satisfactory if proportionate.**

The level of transparency should make retail investors able to assess independently the level of risk. This should include:

- Requirements regarding the prevention of conflicts of interests ;
- disclosure requirements on the usual risks raised by lending-based crowdfunding ;
- disclosure requirements regarding the project, its quality and its risks
- due diligence procedures for projects advertised on the platform ;
- the provision of an appropriate complaints-handling mechanism ;
- internal procedures, especially to address the platform default or failure for ensuring business continuity.

2. Bringing down operational costs and increasing efficiency for the industry

2.5.1 What are the regulatory or supervisory obstacles preventing financial services from using cloud computing services? Does this warrant measures at EU level?

We do not see any specific regulatory or supervisory obstacle that would prevent financial services from using cloud computing services. Outsourcing requirements that must be fulfilled by financial institutions can be accepted by cloud service providers (cf. answer to question 2.6.2).

2.6.2 Should commercially available cloud solutions include any specific contractual obligations to this end?

- ***Yes. Defining a European harmonized framework for cloud computing, applying to the whole financial sector***

The EBA consultation paper “draft recommendation on outsourcing to cloud service providers under Article 16 of Regulation (EU) N° 1093/2010 provides additional guidance to the CEBS Guidelines on outsourcing (2006) for the specific context of banking institutions and investment firms that outsource to cloud service providers. This draft document may become a foundation piece for a European harmonized framework for cloud computing covering not only banks and investment firms but all types of financial institutions. It stresses the importance of contractually securing both the effective right of audit for institutions and competent authorities and the physical access to the relevant business premises of cloud services providers. The document promotes a proportionate approach and provides explanations on how to exercises those rights. For example, small firms, such as Fintech,

can perform pooled audits together with other clients of the same cloud service provider in order to use audit resources more efficiently.

A European harmonized framework for cloud computing, applying to the whole financial sector, could also be a useful supporting tool for financial institutions in the negotiations with cloud service providers.

2.8 What are the main challenges for the implementation of DLT solutions (e.g. technological challenges, data standardization and interoperability of DLT systems)?

- **DLT is a promising technology, but it is still facing some significant challenges**

For the sake of clarity, there are various types of blockchain technology that do not imply the same challenges:

- Some Fintech intend to use public blockchains – and sometimes the cryptocurrency associated, as a kind of universal trust engine and independent money. Public blockchain raises many issues related to governance, anti-money laundering, consumer and data protection
- Some other target "private" blockchains (or Distributed Ledged Technology) or hybrid technologies so as to overcome some or most of the issues related to the public blockchain. It is worth noticing that such restrictions also reduce some of the potential benefits of the blockchain.

Banque de France (BDF) and ACPR are actively involved in the assessment and the concrete experimentation of the blockchain, because:

- As for any firm/administration, blockchain may support the digital transformation of the institution and make business processes more efficient. It is worth noticing the BDF-led MADRE experiment that may be soon effectively implemented: it uses a distributed consensus technology for one ledger that BDF manages, i.e. the SEPA creditor identifier (SCI). The BDF worked in cooperation with several French banking groups provided elements of the software suite and was accompanied by the start-up Labo Blockchain.

- As central bank, regulatory and supervisory authority, blockchain may significantly impact the financial sector (both institutions and market infrastructures) and its supervision. Several proofs of concept (POC) have been conducted or are currently undertaken by financial institutions. They are still not suited to meeting the financial industry demanding requirements in terms of efficiency, availability, safety and robustness, but positive outcomes are appealing for automatizing some parts of financial sector activities that currently rely on manual processes, and conducting business in a more decentralized way.

Nevertheless, DLT is still a very nascent technology; as such several challenges still prevent its development at a larger scale today. We notice the 6 major following challenges:

- Scalability: DLT has mainly been tested in closed environments or for niche activities. DLT for very high volumes or peaks of transactions are less advanced.
- Confidentiality: public blockchain technology does not natively ensure the confidentiality of financial transactions. Thus, observed PoCs turn to closed blockchains, where a trusted party manages access rights. In parallel, some experiments try to prevent some nods from accessing all data, but these experiments are not conclusive at this stage.
- Know Your Customer requirements: blockchain technology can be based on pseudonymisation tools that may be not compatible with KYC requirements

- Diversity of roles (markets participants, CCP, CSD, supervisors): some experiments would like the DLT to be able to grant different access rights, but this approach requires again the identification and the involvement of a trusted party.
- Security: most incidents were not related to the DLT itself but rather to a lack of protection of the access rights. Cryptography incorporated in the DLT help to ensure integrity of the data register but it does not address all security issues.
- Interoperability and standardization: the technologies, protocols and data formats currently used for proof o concepts are very diverse, and this may imply a more fragmented market. Such fragmentation has to be avoided, as important efforts have already been conducted to reduce European markets fragmentation (SEPA, T2S) and are still ongoing (CMU). Interoperability between DLT and with legacy systems has consequently to be supported.

2.9 What are the main regulatory or supervisory obstacles (stemming from EU regulation or national laws) to the deployment of DLT solutions (and the use of smart contracts) in the financial sector?

- ***Banque de France and ACPR welcome any progressive and pragmatic approach that helps to identify and resolve legal and regulatory issues related to the DLT before envisioning its deployment at a larger scale***

We consider that regulation and supervision have to remain technologically neutral. The blockchain technology is still very nascent. Banque de France and ACPR are not aware of mature and sizeable blockchain projects yet. In order to remain technologically neutral, we follow a "wait and see" approach but have engaged at the same time in pro-active dialogue with blockchain players, to understand consequences of the development of such a technology.

The main issues discussed with Fintech that are developing blockchain solutions are the following:

- Reliable customer identification and verification with respect to AML/CFT regulation
- Consumer and data protection, including the right to be forgotten and the quality of advice
- Requirement for Financial Market Infrastructures as far as they are concerned by the projects

In consistency with the neutrality principle, we consider that blockchain technology should especially not decrease regulatory standards with regards those issues.

In particular financial market infrastructures (FMI) have per se strong financial stability impacts. Any regulatory change, if ultimately deemed relevant, has to fulfill international commitments of Members States and European Union and especially the Principles for Financial Market Infrastructures (PFMI) published by CPSS and IOSCO in 2012:

  - Principle 1, "legal basis", stating that Financial Market Infrastructures should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions.
  - Principle 9, stating that central bank money has to be used, when available and practicable, for securities settlement in a delivery versus payment mode. For Euro, this means that those DLT-based services aiming at providing securities settlement have to connect to Target 2 Securities, either indirectly via an already connected CSD, or directly, meaning that they have to obtain a CSD authorisation under CSDR.

The French government is currently working on a legal framework for the use of DLT for the management of unlisted securities. Whether the DLT is used to solely perform tasks that are

today endorsed by classical IT tools (securities accounts that today serve as proof of ownership and legal representation of securities) or the DLT implies fundamental changes in the financial activity (endorsing for instance the cash transaction), will determine the magnitude of the change. It should allow the DLT to be lively tested on well-identified niches before thinking about scaling up the technology. Beyond issues stemming from financial regulation, potential legal issues raised by the blockchain may also come from contract law or property law.

3. Making the single market more competitive by lowering barriers to entry

3.1 Which specific pieces of existing EU and /or Member State financial services legislation or supervisory practices (if any) and how (if at all) need to be adapted to facilitate implementation of Fintech Solutions?

- ***Licensing new credit institutions: further analyze the merits of a sequencing approach***

In a recent consultation[1], the EBA considered whether the regulatory technical standards for the authorisation of credit institutions should introduce a sequencing licensing process in order to allow new banking start-ups to submit information in a sequenced manner in order to allow for a limited authorisation for start-ups during an interim period. There are many ways in which such a process could be structured. For instance, and without lowering the quantitative /prudential requirements set up by CRR, a restricted license -with meaningful restrictions (such as a low overall cap for the amount of deposits and basic credit activities to lower risk profile) could be granted for a set period of time, based on an application file focused on the core requirements applicable on business plan, management, governance and control and a plan setting out when and how the remaining requirements are implemented (policies and procedures, outsourcing arrangements, recruitments…).

Finally, the EBA decided not to develop in more detail such a framework, partly because CRD4 does not specifically refer to such a process and limited or interim authorization could create confusion or diminish confidence in the standing of credit institutions in the EU. The EBA also mentioned that it remains to be assessed whether there is a significant need for such a process, considering so-called FinTech companies would not necessarily seek to become full-blown credit institutions.

The EC could consider whether or not it is worth developing further work in this area, taking into consideration the potential feedback received by the EBA on this issue (see question 8 of the EBA public consultation) and other work to be done on the proportionality in banking supervision.

- ***Digital on-boarding: need for EU harmonization***

Digital or electronic identification and identity verification are not harmonized in the EU. Therefore, financial actors, especially fully digital actors could face difficulties to expand their activity in other EU countries, since they have to comply with different national regulations for remote customer onboarding. Banque de France and ACPR would encourage further EU efforts towards harmonization in this significant area, to establish an EU standard on remote but secure means for identification and verification that would be equivalent to face to face. The provisions already in force with eIDAS Regulation should be particularly examined to this end.

[1] European Banking Authority - 8 November 2016 - Consultation on RTS and ITS on the authorisation of credit institutions (EBA-CP-2016-19)

3.2. What is the most efficient path for Fintech innovation and uptake in the EU? Is active involvement of regulators and/or supervisors desirable to foster competition or collaboration as appropriate, between different market actors and new entrants? If so, at what level?

- ***The ACPR Innovation Hub has struck the right balance between innovation, regulation and financial stability***

The ACPR (French banking and insurance supervisor), as well as the AMF (French financial market regulatory agency), has set up a dedicated Fintech Innovation Hub (in French *Pôle Fintech-Innovation*) to provide innovative financial players assistance and more clarity about the financial regulatory framework. This Innovation Hub addresses one of the most pregnant barriers to entry for FinTech, which lies in the spread and the knowledge about financial regulation, which may sometimes be very complex, especially for entrepreneurs that did not work in the financial sector before. The Innovation Hubs is open to all type of players because innovation can be driven by all types of players. There is no specific process for entering in contact with the Hub, because ACPR favors informal and reactive dialogue with the Fintech.

Since the launch of the Hub in June 2016, more than one hundred of financial players have been proposed with meeting or a call with the Hub. The level of advancements of projects varies a lot but ACPR experience is very positive and we deem that we have reached the right level of engagement for supporting the Fintech development.

In addition to the day-to-day dialogue with Fintech, the Fintech ACPR team aims at ensuring and promoting (i) agile regulation because technologies and market practices evolve very rapidly, (2) effective proportionality of rules and supervisory practices because regulation must be driven by the scale of risks (3) and oriented-to-effectiveness regulation. Through active dialogue with the Fintech community and other public authorities, ACPR can contemplate and propose regulatory changes and supervisory adjustments. Since the ACPR Innovation Hub welcome Fintech projects at early stages, it is also able to identify promptly evolving market practices and new business models that may give rise to future regulatory and supervisory issues.

3.3. What are the existing regulatory barriers that prevent FinTech firms from scaling up and providing services across Europe? What licensing requirements, if any, are subject to divergence across Member States and what are the consequences? Please provide details.

Fintech invest in the full range of financial services (financing, payment, investment, and insurance). It is difficult to identify as such regulatory barriers in all areas where Fintech innovation happens. Against this background, we focused our remarks on 3 issues ACPR is facing including 2 on the field of payments, where a lot of Fintech are present:

- ***Frontier between e-money and payment services: merging payment and e-money directives***

With innovation in the payments area, the frontier between e-money and payment services is blurred. The e-money directive (EMD2) was designed in 2009 mainly to regulate physical prepaid cards. With many innovations in the field of electronic money, the frontier between Payment Services Providers and e-money has become unclear and raised interpretation issues when licensing such services. At European level, we have also noticed diverging interpretations by National Competent Authorities (NCAs) regarding similar products. Such qualification entails some consequences in term of prudential requirements as well as AMLD-

CT requirements. Against this background, many NCAs were in favor of merging PSD and EME when discussing the new PSD2. We understand that it was not possible to do so due in particular to lack of impact assessment of EMD2. Since the revision of EMD2 should have taken place more than 5 years ago, ACPR and Banque de France suggests reviewing the EMD2 regulation as soon as possible in order to clarify the concept of e-money and improve the alignment of the EMD2 with AMLD-CT regulation.

- ***Payment institutions licensing requirements: need for further harmonization***

In relation to licensing requirements, the recent updated regulations and related RTS improved significantly the harmonization of licensing expectations among EU regulators. Some supervisory convergence work is however required within ESAs. In the payments area for example, PSD1 and PSD2 foresee three different methods to calculate own funds requirements. Such method should be selected by each Competent Authority, but with no specific guidance on how to do so. Again, such option has significant consequences about the own funds requirements, which can lead to divergences across Member States.

- ***EU convergence about peer-to-peer insurance would be needed***

Some projects relating to the so-called « peer to peer insurance » have been presented to the ACPR during the last two years. We should make a distinction between:

- Some kind of cashback system, based on the actual claims observed on a predefined community, embedded in a traditional insurance scheme, which are therefore quite suited to the current insurance regulation
- More innovative business models where the predefined community uses a kind of pooling outside the insurance universe, with or without a top guarantee from an insurer if the pool is exhausted. As these models are frequently close to the limit between intermediation, insurance and payment services for money pots, their regulatory treatment amongst European NSAs could be inconsistent, and a clarification at a European level would therefore be welcomed.

3.5. Do you consider that further action is required from the Commission to make the regulatory framework more proportionate so that it can support innovation in financial services within the Single Market? If so, please explain in which areas and how should the Commission intervene.

- ***Launching an overall reflection on the regulation of financial intermediation***

We can see that new business models are emerging: aggregators are turning into multi-services platforms, combining account information services and payment initiation services under PSD2 but also advisory services for insurance and investment products. Access to consolidated customer payment data will support new advisory practices based on innovative uses of data. Some of these platforms would also like to offer usual payment services (payment account, debit card, transfers etc.). They could also want to be registered as intermediaries in banking transactions (in French "*Intermédiaires en Opérations de Banque et en Services de Paiement*", IOBSP: national status). These platforms combine national and EU status that were probably not designed to be used all together. It is therefore really complex to understand how to combine (or not) some of those status and how the different set of rules can work together. These issues are currently discussed with the French Innovation ecosystem in the ACPR-AMF Fintech Forum.

We stand ready to discuss with the EC the regulatory challenges raised by those digital platforms to assess whether there is a need for a further action in this area.

- ***Market shares of credit platforms remain so far limited, but this is an area where further action may be needed in the future***

For crowdlending activities, there could be benefits to think about, when the market is more mature, a common and harmonized European regulatory framework to support the further development of credit platforms at the European level. However, such a framework should take into account the prevention of regulatory arbitrage across the EU, by redefining the field of free provision of services and by giving the host authorities more power regarding rules of conduct of the intermediaries and customer protection, as regards activity realized with customers living on their territory.

- ***EC's and ESAs role***

Against this background, EC and ESAs should continue to monitor of innovations at EU level, analyzing whether and how such innovations may challenge current regulations and suggest evolutions of the regulatory framework if needed. This approach was followed by the EBA for example in the field of crowdfunding (EBA/Op/2015/03), virtual currencies (EBA/Op/2014/08) and innovative uses of data (EBA/DP/2016/01). When an evolution of regulation is required, a greater involvement of ESAs in this process could improve the present situation.

3.7 Are the three principles of technological neutrality, proportionality and integrity appropriate to guide the regulatory approach to the FinTech activities?

- ***Yes. Banque de France and ACPR agree with the EU Commission principles to guide regulatory approach to Fintech: technologically neutral, proportionality and market integrity.***

- Technology neutral because innovation can be driven by all types of players and regulatory agencies may be neither legitimate nor able to identify and select innovative projects. As regards the emergence of new technologies and new business models, agile regulation is also needed: regulatory adjustments can be contemplated (including regulatory simplifications) and "test and learn" initiatives can help preparing the future of financial regulation. For instance, the French law acknowledges now the blockchain technology for the register on non-listed equities. Based on that first live experiment, the blockchain technology could later be acknowledged for an extended scope of services.

- Proportionate because the level of regulation and supervision must always be proportionate and driven by the consideration of the scale of risks (in that area not only prudential regulation must be considered but also data protection, consumer protection and AML/CFT regulation). This approach should allow softening the entry of new players in the regulatory scope (license waivers or sequencing process for getting the full license). Rather than being too prescriptive or detailed, principle-based regulation is also likely to effective and more adequate in very innovative environment.

- Market integrity provided this principle clearly encompasses (1) consumer protection including data protection, (2) AML/CFT, (3) market security (including security of payments) and (4) financial stability

These principles need to be based -as far as possible- on a more holistic approach of the regulation applicable to the financial sector, in order to take into consideration all the impacts of the digital revolution (financial stability, customer protection, AML/CFT, data protection, cyber risk etc.) and to build a consistent digital regulation.

3.8.1 How can the Commission or the European Supervisory Authorities best coordinate, complement or combine the various practices and initiatives taken by national authorities in support of FinTech (e.g. innovation hubs, accelerators or sandboxes) and make the EU as a whole a hub for FinTech innovation? Would there be merits in pooling expertise in the ESAs?

Based on the positive feedback received from Fintech, Banque de France and ACPR deem that Fintech are asking for close and simple dialogue with their national authorities and appreciate to get answers in a timely manner. Various avenues could be explored to promote further cooperation between member states:

- At the sectorial level, the **ESAs** could play a key role in the sharing of information between national authorities so as to (i) help identify key features of Fintech observed in the different jurisdictions, (ii) favor a common understanding of the stakes their raise from a supervisory perspective and (iii) shed light on developments having cross border implications. This approach would pave the way for the development of convergent responses across countries, whenever relevant. In doing so, the ESA would have to strike the right balance between complementing the role of NCA and preserving the benefits of local setting which have been put in place to handle Fintech. The pooling of expertise seems to be a good solution, but more in the form of network than through centralization; In parallel, the **Joint Committee** would in addition need to deal with trends having potentially or actually cross-sectoral implications, be they related to entities or to products.
- As to the **Commission**, there might be some merit in fostering the cooperation between different authorities. A typical examples (among many others) lies in personal data protection topics (such as those linked to the use and storage of biometric data), Indeed, PSD2 favors the open banking and open data principles for payment accounts, what potentially increases the risk for the data protection (consumer protection and market conduct). Thus, ESAs could engage further cooperation with G29 in this area.

3.9 Should the Commission set up or support an "Innovation Academy" gathering industry experts, competent authorities (including data protection and cybersecurity authorities) and consumer organisations to share practices and discuss regulatory and supervisory concerns? If yes, please specify how these programs should be organised?

- ***Yes. Banque de France and ACPR would welcome an Innovation Academy at EU level and stand ready to participate in such a forum***

The Commission is well placed to gather various stakeholders. An “Innovation Academy” could be a suitable way to do so. As a matter of inspiration, the FinTech Forum created by the ACPR and the AMF gather FinTech, banks, insurance companies, investors, academics and Public Authorities (Ministry of finance, data protection Authority, Tracfin the French Financial Crime Unit, ANSSI French national agency in charge of information systems), so as to make sure that the policy proposal are discussed with various stakeholders concerns and effectively adapted to the challenges raised innovation.

Based on this positive experience, we recommend this Innovation Academy to be open to the whole financial industry (both Fintech and incumbents) so to be able to understand the regulatory challenges raised by innovative technologies and new business models. It should

also be accessible to representatives of other European public authorities in charge of data protection (G29), cybersecurity (ENISA) or AML/CFT (EU Financial Intelligence Unit platform). Its composition would need to be flexible in order to adapt the stakeholders to the topics and its agenda would need to be co-built in an open and cooperative way.

3.10.1 Are guidelines or regulation needed at the European level to harmonise regulatory sandbox approaches in the MS?

- ***Banque de France and ACPR think that the term of "sandbox" should be considered cautiously, because it does not benefit from a clear and consistent definition.***

- Sometimes, sandboxes mean that new financial technologies should develop outside any regulation (e.g. "non-action letter" issued by the supervisor, which even occasionally issues calls for proposals to FinTech project holders wherein it selects the preferred ones) or benefit a tailor-made derogatory regulatory regime. This approach may raise several concerns :
    - We doubt that supervisors would be legitimate to identify and select innovative projects, without involving by-side negative effects;
    - There may be some questions about the duration of such a sandbox and as to how innovative projects to get out of that derogatory regime and enter the regular regulation (threshold effect);
    - This kind of approach may raise level playing field issues with incumbents.

- Sometimes, sandboxes can mean that innovation should be supported by tailored and pro-active supervision of innovative projects (reinforced and constructive dialogue project holders). Although the term sandbox is confusing and misleading, it may basically mean "sound regulation", which is actually the proportionate approach French regulators support and implement in France. It gives the same chance to every FinTech project holders whatever their regulatory framework.

3.10.2 Would you see merits in developing a European regulatory sandbox targeted specifically at FinTechs wanting to operate cross-border? If so, who should run the sandbox and what should be its main objective?

Yes. Banque de France and ACPR notices that the majority of Fintech project holders can find a suitable status within the current financial regulatory framework, even if the proportionality principle may be improved in some areas.

But when the innovative project is likely to be disruptive and cannot fit with the existing regulatory framework, the EU could assess the need of setting up a sound regulatory regime for experimentation and testing in real conditions in the financial industry. For instance, DLT solutions raise significant legal challenges such as: the legal value of a digital asset of a digital register, of a smart contract, of a digital transaction etc. Such a European initiative could foster innovation in the European financial sector. Such a test and learn approach could also be helpful to prepare the regulation of such a very innovative solution. Since the financial industry is essentially regulated at EU level, an EU initiative would be more legitimate and meaningful than the multiplication of national approaches, which may impair the consistency and efficiency of EU financial regulation.

4. Balancing greater data sharing and transparency with data security and protection needs

4.7 What additional (minimum) cybersecurity requirements for financial service providers and market infrastructures should be included as a complement to the existing requirements (if any)? What kind of proportionality should apply to this regime?

In order to become reliable and trusted parties in the financial space, Fintechs need to ensure they offer secured services and protect clients' information with up-to-standards solutions. Fintechs sometimes bring innovative security solutions which can become standards for the financial industry. But there could also be situations where, being start-ups, Fintechs do not have fully-secured environments. In this respect, it has to be noted that supervisors expect financial institutions to ensure the security of their information systems in the most comprehensive way, since attackers might always benefit from an inadequate security level of a peripheral IT system to gain progressively access to a sensitive and secured core system. It is therefore important to have Fintechs applying security measures in a comprehensive manner also. It should lead to the use of measures aiming at preserving the confidentiality (e.g. cryptography for sensitive data storage and transit), the integrity and the availability of data and systems. This does not prevent the application of the proportionality principle, since Fintechs' IT environments are usually smaller and easier to control.

As regards specifically payment services providers (PSPs), the introduction of two newly regulated services (payment initiation and account information) by the 2nd Payment Services Directive (PSD2) requires an access for new actors (third party providers, TPPs) to the accounts held by other PSPs. In order to prevent potential cyber threats on this access, Regulatory Technical Standards prepared under the aegis of the European Banking Authority define the minimum security requirements for the communication interface between PSPs. These requirements should definitely aim at (i) eradicating any insecure practice such as webscraping (i.e. the TPP uses its client's personal security credentials to access to the public e-banking website of the PSP) which use is in contradiction with security provision laid down in PSD2 even as a "fallback solution", and (ii) favouring the implementation by all actors of innovative solutions presenting the most adequate –and cyber resilient– security level for TPPs' access as designed by the EBA.

As regards financial market infrastructures, notwithstanding used technologies, they already have to comply with specific requirements on risk management that are contained in the PFMI published by CPMI and IOSCO. They have been specifically complemented by a dedicated guidance on cyber resilience that could become a useful reference for other financial institutions. Accordingly, it is of utmost importance to ensure the resilience of any component, including the non-core components that could be less secured as considered less strategic, and as such being easy targets for hackers. It has to be underlined that consequently, the usual sense of proportionality is both outdated and inappropriate as far as cyber security for FMI is concerned.

4.8. What regulatory barriers or other possible hurdles of different nature impede or prevent cyber threat information sharing among financial services providers and with public authorities? How can they be addressed?

- ***Defining an homogeneous taxonomy for cyber incidents***

Information sharing on cybersecurity implies trustworthiness among the different parties. Public authorities have a role to play in order to organize such secure and trusted information

sharing. Moreover, information sharing is key to enhance cyber security measures and controls.

However they are currently different frameworks in place at national and international levels, which may lead to various and non-aligned exchanges. Besides, private actors might also want to develop information exchanges.

Banque de France and the ACPR are not pushing for additional exchanges platforms and are ready to contribute to enhance the homogenization of the different incident reports that are starting to be put in place (or about to be put in place) in order to favor consistency and reduce the burden for market players. In this respect, it is important that regulators help defining a taxonomy of cyber-incidents. This will facilitate communication, comparisons between sectors, as well as to seize the importance and trends of the threats.

4.9 What cybersecurity penetration and resilience testing in financial services should be implemented? What is the case for coordination at EU level? What specific elements should be addressed (e.g. common minimum requirements, tests, testing scenarios, mutual recognition among regulators across jurisdictions, of resilience testing

It is commonly agreed that cyberattack could affect any actor, which makes the case for penetration testing. As cyber resilience is not only a technical issue, different levels of testing should help discover and address as many potential flaws as possible in the domains of governance, identification, protection, detection and resumption/response/recovery. Basic penetration testing is thus as important as table exercises and red teaming.

With the help of Banque de France, the ACPR could develop a supervisory practice of penetration testing as part of its on-site inspections. This practice, associated with a comprehensive and detailed review of the IT security, allows the supervisor to appreciate concretely the quality of the defenses that the licensed institution has in place. This approach is targeted, since it intervenes in the course of investigations performed on one licensed institution. It is not a market place approach like the Bank of England C-Best program. The merits of the ACPR' approach is that it does not imply the recourse to external resources and that it is adapted to the individual situations.

In addition, the Eurosystem is currently working to establish a red teaming penetration testing framework for financial market infrastructures. Elements that will be addressed are:

- Engagement between regulators and stakeholders at the international/national level
- Scoping
- Procurement
- Threat intelligence
- Red teaming organisation
- Remediation planning
- Results sharing