POSITION PAPER

ESBG's reflections on the Commission FinTech Action Plan

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

Transparency Register ID 8765978796-80

22 June 2018

ESBG

I. General

ESBG welcomes the Commission FinTech Action Plan. It is particularly welcome that through this plan the European Commission seems to acknowledge the importance of an approach to defend the sovereignty of Europe in the digital field, stating: "[…] *Europe should become a global hub for FinTech*".

As a vital underpinning to all information contained therein, we especially support the definition of FinTech as "technology enabled innovation in financial services". It is important for levelling the playing field as financial institutions who provide a comprehensive range of services such as ESBG members have been active innovators in their own right for a long time. ESBG members have an interest in FinTech, and they make use of many existing FinTech solutions by investing in Financial Technology (FinTech) or via partnerships with other FinTech firms and start-ups. Moreover, using the term Fintech, as often done, in the sense of "start-ups", is confusing. Considering FinTech firms as different entities can lead to misjudgement in terms of defining a regulatory approach to FinTech activities. It needs to be asserted that FinTech can be provided by either financial institutions such as savings and retail banks as well as new entities focusing on a specific activity in the supply chain that characterizes the financial sector.

A prerequisite for the future of financial innovation and a level playing field is to ensure both consumer protection and financial stability. Therefore, it is necessary to maintain technological neutrality and a level playing field horizontally across regulation and across Members States - addressing issues such as KYC, digital on-boarding, electronic identification, capital requirements and transparency.

If we want to properly estimate the stakes, the various players on FinTech should be designated precisely: incumbent banks, start-ups and the American and Asian Web giants. We believe that the common goal of all European stakeholders (institutions and market players) should be to prioritize innovation in order to give birth to European leaders (and consequently to be able to compete with BigTech from the US and Asia).

II. Proposal of the Crowdfunding and Crowdlending Regulation

ESBG's position on this is quite simple: Crowdfunding and peer-to-peer lending platforms should abide by the same legislative measures as banks. The European Commission's inception impact assessment in November 2017 outlined four possible options to develop the EU crowdfunding sector. Both option 1 (baseline scenario: no EU framework) and option 2 (self-regulatory approach with minimum EU standards) were dismissed by the Commission and ESBG.

Some ESBG members support option 3: A comprehensive EU approach – treating platforms like regulatory trading venues or payment institutions. This approach secures a level playing field, enabling platforms to scale cross-border, and at the same time securing reliability and trust through a proportionate and effective risk management framework. At the very least, European crowdfunding and peer-to-peer lending platforms should be subject to the same rules as incumbent financial institutions offering similar banking/financial services in the following areas:

- Consumer protection/Investor protection
- Anti-Money Laundering
- Capital Requirements associated with operational risk
- Risk management
- Banking secrecy
- Information disclosure

- Fair and transparent contract clauses and fee structure
- Data protection and compliance
- Authorisation or registration of the crowdfunding platform
- Supervision and monitoring of regulatory compliance.

In addition, activities related to payment initiation/aggregation and crowdfunding/lending should not be able to be combined. If a system combines payment initiators/aggregators and crowdfunding/lending platforms, for example as hybrid payment institutions, these institutions could use their platforms to provide their customers with banking information from various institutions (which must allow this), manage their payments and provide them with both financing and investment opportunities through crowdfunding/lending. These institutions could therefore provide practically the same services to their customers as a credit institution, without in turn offering the same guarantees related to solvency, governance and consumer protection.

The European Commission's aim to develop a proper legal framework for crowdfunding across the EU, as an optional label for crowdfunding service providers, is a good first step toward harmonisation. Potential areas of harmonisation include crowdfunding platforms' disclosure requirements, registration requirements, risk management and consumer / investor protection rules.

In the long term, ESBG considers that EU legislation should evolve toward a full harmonisation of practices in order to ensure a level playing field among platforms. National platforms could gain a regulatory advantage compared to cross-border platforms due to potential less-demanding local regulations. Furthermore, a lack of reliability in local platforms operating below 'best practice' standards could have a negative contagion upon the trust in cross-border platforms. Finally, existing regulations of credit institutions, credit intermediators and investment firms should be taken into account in order to reflect the nature of the platforms different services and nature.

Above all, we think that the ultimate goal for a regulatory approach must be maintaining a level playing field. One important factor to be taken into account is that a bank should not bear the risk for activities of crowdfunding companies. Yet, this approach may be adapted towards the specific relationship between partners, e.g. depending on whether or not the crowdfunding company being only a vendor and the bank keeping the relationship and the profit & losses in its own books versus the bank being only a lead generator.

III. FinTech, the PSD2 and the GDPR

ESBG supports the Commission initiative to address identified regulatory gaps and will contribute to the best of its ability in this respect. Regarding the adoption of APIs compliant with the GDPR and the PSD2, ESBG would like to point out that we are currently in the process of identifying all of the inconsistencies/clashes between the two legislative acts. It is perceivable that some of this has and will continue to become apparent after the entry into force of the GDPR. All of the eventually identified issues will be communicated to the Commission in due time. With respect to API developments currently going on, ESBG would like to reiterate that API functionality should comply with the requirements as stipulated in PSD2, the related RTS and the GDPR only, and that API functionality should be benchmarked against this legislation only. Requirements that go beyond what is legally required should not be taken into account by the National Competent Authorities and the EBA when assessing APIs. Moreover, we feel that the information available to be provided to TPPs should be limited to payment services and accounts based on the PSD2 (excluding, for example, information about financial instruments or insurance policies).

IV. Expert Group to review the fitness of the EU financial services regulatory framework

ESBG advocates a regulatory approach that would result in less regulatory constraints to financial innovation based on the principle of same services and risk, same regulation. We support such an initiative and have nominated representatives to the above mentioned Expert Group.

V. The EU Blockchain Initiative

Savings and retail banks throughout the EU have taken great strides to acclimate themselves to the digital transformation. The most recent development in this ongoing process is distributed ledger technology. As this topic is of interest to us, ESBG will endeavour to provide input in the planned consultation and will follow the Commission's activities.

In general, we would appreciate a fluid discussion with the EU experts; key documents or other information could be circulated via the various associations, e.g. ESBG, to give their members a better idea about the discussion in the different expert groups.

We would like to stress that a quick know-how building of competent authorities should take place at both levels, the European one but also the national one.

Furthermore, we would like to point out the following obstacles concerning DLT technology that we have identified so far:

- Absence of the existence of different legal frameworks for General Terms and Conditions/B2C-B2B-Contracting in general and in particular, regarding Smart Contracts ("Code as Contract")
- Different Data Protection Laws (EU and national ones) for personal data exchange especially cross-border (they serve as the basis for contract initiation and crime prevention)
- No Data Standards (ISO20022 could serve as a basis, but there is no European initiative, consequently US/China may take the lead)
- No standardised definitions for common contracts (terms and conditions, payment, digital freight papers, digital signatures/authentication/authorization/identification, collaterals/access to company/land registers, etc.)

VI. Crypto-assets and ICOs

ESBG welcomes the continuous development assessments of crypto-assets and Initial Coin Offerings (ICOs), in particularly the application of the EU financial markets regulatory framework to these new assets or services. Because of their similarities on many aspects with traditional assets or services (financial instruments and Initial Public Offerings), it is paramount that, on the one hand, investors benefit from an equally high level of protection, and, on the other hand, a regulatory level playing field is ensured. To achieve this, the following risks require regulatory actions:

- Regulatory uncertainty on ICOs leaves room for a growing part of the economy remaining in a regulatory limbo that helps new firms flourish at the expense of heavily regulated competitors, while leaving investors without any protection.
- There is also growing risks stemming from the impact cyber-attacks can have on the ICO market. For instance, when a trading platforms have their crypto-currencies stolen or when an ICO appears to be a scam and is allowed to go through.

- The lack of due diligence performed by the firms behind ICOs and the lack of identification of anonymized investors allows a high degree of speculation and market manipulation; through techniques, such as, dumping, spoofing, front running or whales.
- That high level of anonymous cryptocurrency trading also raises related AML risks.
- Smart contracts as a basis of the technology behind ICOs are not as developed as the foundations of traditional markets. See for example the case behind the now defunct DAO.
- The uncertainty on the value of tokens pre- and post-sale increases risks of price volatility.
- Finally, there is a significant lack of clarity regarding the fiscal rules applying to tokens raised through ICOs.

In order to best tackle these risks, it is necessary to organise regulated markets for crypto-tokens that offer guarantees in terms of: price transparency; submitting traders; platforms or issuer of crypto-tokens to AML regulation; copying rules on market abuse/manipulation to trading platforms for cryptocurrency, and minimal information disclosure. We believe that at the minimum a clear regulatory framework is needed on those issues.

If not, consumers/investors may find it particularly challenging to bring any crypto-token-based revenues into the ordinary financial system. Specifically, we feel that regulators should thoroughly review the AML risks associated with the various stages in a crypto-asset lifecycle, and related activities, and provide clear direction as to their treatment. For example, within the KYC processes, promoting a safe adoption by all players.

The associated consumer protection issues primarily stem from the lack of a globally consistent view on how this novel product should be classified, i.e. falls under an existing financial instrument category or requires a new definition/category. As a result, consumers suffer from the lack of consistent protection. Fragmented regulation, even at the regional level, complicates this issue further. To address this issue adequately, global coordination and alignment is needed to effectively address these globally active products

It seems also important to be able to categorise the nature of tokens. Depending on this nature, different regulations could apply. Sharing a common taxonomy of tokens could help all stake-holders to have a better understanding of the diligence associated therewith.

Moreover, we are of the opinion that those additional issues require actions from authorities at EU level; setting up external audit requirements for firms issuing tokens through ICOs as well as initiatives regarding education and digital skills both from the investor and regulatory authority.

VII. Cybersecurity

ESBG welcomes the public-private workshop planned for the second quarter of 2018. Moreover, we would like to take this opportunity to express some of our views on cybersecurity.

Service providers must constantly adjust and refresh measures designed to protect data to mirror the constantly evolving technology and thus new threat profiles. Cybersecurity, focusing on data privacy, needs to be a prioritised issue for public private dialogue going forward. It is important to, not only work for the stability and longevity of the financial system but also the integrity of European citizens.

Cybersecurity should not be treated nor regulated with proportionality criteria. Cyber-attacks must be prevented not from happening to the largest companies, but to all of them. As the European Parliament stated in its FinTech Report, "a connected system is only as safe as its weakest element",

and due to the interconnectedness of the financial sector, it will be critical that all service providers ensure the same level of cybersecurity. Therefore, any potentially new legislation should be assessed against the risk of altering the level playing field, meaning that only some players should not be required to invest disproportionately in order to counter the new risks imposed on their supply chain across the Union.

Furthermore, we believe that on the prevention side, the role of digital literacy, skills and awareness should be acknowledged and promoted. We also find best practice documents at industry level to be useful if updated regularly. However, we emphasise that the precondition for this are trusted real time channels for the exchange of relevant information. This should therefore be encouraged. With respect to detection, we feel that financial institutions should be rest assured that any information they voluntarily share with government on cyber threats will remain confidential. Finally, we believe that enforcement authorities including police forces should be compelled to investigate cyber-attacks with much greater priority, whereas cooperation with bodies outside the EU should be encouraged.

Moreover, given the importance of the stability of the financial industries' infrastructure to the European economy we believe that the Commission should establish a European Centre for Cyber Security in Banking and Finance. Similar to the one established for Aviation (ECCSA).

Finally, we would like to point out the following minimum cybersecurity requirements we are recommending:

- The uncompromised infrastructure principle, i.e. end-to-end evaluation of infrastructure security checks/detection requirements (from end-user device over internet connection to service-provider infrastructure and onward to outsourcing-/business-partners).
- Each infrastructure line and point has to be protected directly via root-checks/malware-checks/etc. and indirectly via behavioural analysis/etc.
- Qualification of acting security managers has to be proven (e.g. international certifications – CISSP, CISM, CRISC) – they should speak the same "security" language
- Security principles (Security by default, Security by design)
- Secure Software development
- Cyber Threat Intelligence
- For Cybersecurity penetration and resilience testing, a minimum EU standard should be defined
- To save time the best existing national standard of a Member State should be chosen and brought on EU level (e.g. CBEST from Bank of England)
- Tester should be certified on this minimum EU standard (already done by Bank of England)
- Management attention should be brought to EU wide resilience exercises
- Participating in EU wide Cyber exercises should the coupled with incentives for the organization by the regulator

These requirements could also work as a base for the work done in the various market-led Application Programming Interface standardisation initiatives that are in the process of developing APIs that are compliant with PSD2 and GDPR.

VIII. Digital Skills

ESBG welcomes the Commission's emphasis on improving digital skills as highlighted in the 2018 Digital Education Plan. An estimated 44% or 169 million Europeans do not have basic digital skills

and the need for media literacy and a variety of digital skills and competences including safety, security and privacy is constantly growing. To fulfil this need, education and training systems should develop digital technology related programs as well as encourage the development of relevant digital competences.

In its September Communication on cybersecurity, the Commission called on EU Member States to pledge to include cybersecurity in academic and vocational training curricula, in particular at early stages. The role of digital skills and awareness should be acknowledged and promoted, as informed citizens and consumers are better placed to identify cyber-attacks. In this regard, ESBG welcomes the Commission's continuous reform efforts, such as the recent adoption of the new proposal on Key Competences for Lifelong Learning, as well as the various initiatives put in place, in particular the Digital Opportunity traineeship scheme. Many of the financial education initiatives of ESBG members already encompass a digital dimension, thus helping to enhance the digital skills of the addressees. An example of this is the European Stock Market Learning Initiative, a European initiative aimed at enforcing young people's literacy in business and financial affairs through an online simulation of financial investments. In addition to those initiatives, we consider that the UK's HM Treasury's "FinTech Sector Strategy" provides diverse examples of good practices in the area of digital skills. For instance, to cite some, the new Computing Curriculum, the introduction of new T-Levels with Digital contents, the launch of a new Institute for Coding, or the set-up of a new Advanced Maths Premium fund to help schools and colleges increase the number of students studying math.

Moreover, it is also relevant to ensure that cross-sectorial firms have access to the right digital skills. The established retail banking community currently finds different hurdles for attracting FinTech talent. In this case, for example, a good practice can be seen at the UK's "Tech Nation visa scheme".

Nevertheless, a persistent digital divide exists between and within EU Member States. Narrowing the digital divide and addressing digital exclusion is also part of the mission of all stakeholders in society. In this respect, embers of the savings and retail banking community are contributing their share through multiple forms of engagement, notably through their delivery and support channels.

As digitalisation affects the day-to-day lives of all citizens, some jobs will disappear, others will be replaced, new jobs will be created, many jobs and industries will be transformed and new activities will emerge. Investing in one's digital skills throughout life is therefore paramount. Around 90 % of jobs nowadays require some level of digital skills, yet 37% or 93 million in the labour force do not have basic digital skills. If we fail to acknowledge the ever increasing importance of digital skills, Europe risks losing its most competitive edge — a highly-skilled and educated workforce. We would like to point out that in the context of the Sectoral Social Dialogue in the Banking Sector, ESBG and the social partners have been leading a twofold project focused on The Effects of Regulation on Employment in the Banking Industry. Pillar I of this project, consisting of data collection on the employment situation in the banking industry within the EU 28, is soon to be finalised. Pillar II will then list and evaluate the impact of adopted regulations on employment. Furthermore, ESBG has recently committed to promoting a joint declaration on the social effects of digitalisation, proposed by UNI Europa.

IX. The free flow of non-personal data

We would like to take this opportunity to also address some concerns we have with the Commission proposal for the Regulation on the free flow of non-personal data. Namely, our concern is that the "national security" restrictions are counterproductive with respect to the aims of the regulation.

IX. Artificial Intelligence / Machine learning/ Robo advice

Considering that Artificial Intelligence/Machine Learning will have a more far reaching and immediate impact on banks than all other technologies together (big data, cloud, distributed ledger technology, biometrics, etc.), we would appreciate an EU approach in this perspective. When adopting such an approach, we would appreciate if it took into consideration the following:

- AI and machine learning can increase accessibility to new segments of customers because it provides a better picture of the user's needs. For instance, the use of AI in a robo-advisor model helps to reach younger customers with simple needs, or with small accounts that want to start to invest. In addition, from a cost efficiency perspective, it allows for a reduction of operational costs once the initial developments are amortized.
- EU-policies should be technology-neutral: The same activities should be subjected to the same regulation irrespective of the way that the service is delivered, so that innovation is enabled and a level playing field preserved. Therefore, no specific regulation applying to financial institutions with respect to AI or machine learning should exist, as it could be unfairly harmful for the financial services industry requiring to meet stricter requirements than other industries for the use of the same technology. Classical "on-site" advisory services must not be put at a disadvantage, more so when currently most Member States offer comprehensive on-site advisory services to customers, which provides for appropriate access to finance.
- If the EC is going to establish a regulation/supervision for all the economic sectors using this technology, the supervision should include a combination of a set of minimal rules and ongoing assessment. Internal controls and governance mechanisms can be designed to guarantee financial stability, along with a constant dialogue and interaction with supervisors to assess the performance of these tools –which should be on the other hand designed according to the entities' risk appetite framework and to the different internal policies and procedures and validated by the supervisor. In addition, the oversight should not focus on the supervision of the algorithm that is at the end of the process, but on the dynamics of the root artificial intelligence engine that has generated the algorithm. For this, it is necessary that supervisors and regulators have among their human resources some specialists in artificial intelligence to exercise proper oversight.
- From the point of view of transparency, we do not believe that it is convenient to disclose how the algorithms work; they are a source of competitive advantage for entities' business models and this could be put at risk.

Therefore, we welcome the set-up of an Expert Group to review the fitness of the EU regulatory framework involving discussions at national level.

X. Sandbox / Innovation Hubs

We are of the opinion that supervisory cooperation in this matter would be of utmost importance. Respective guidelines, standards and EU regulatory support would be appreciated. The objective of a regulatory sandbox should unambiguously be to establish a customised regulatory environment to allow both newcomers and incumbents to pilot on a small scale, and it should be stressed that the sandbox is not lowering regulatory standards, as consumer protection is paramount. We feel that the proposed "learning from each other" approach would not be sufficient. National solo approaches in all of the areas covered by the sandboxes only create a difficult regulatory environment and foster fragmentation of the EU FinTech market. Due to the lack of an EU-wide approach, national initiatives still have their reasoning. However, in order to promote the Digital Single Market, the creation of an

EU Innovation Hub or sandbox by the European Commission, as a single contact point is highly recommended.

About ESBG (European Savings and Retail Banking Group)

ESBG represents the locally focused European banking sector, helping savings and retail banks in 20 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 1,000 banks, which together employ 780,000 people driven to innovate at 56,000 outlets. ESBG members have total assets of €6.2 trillion, provide €500 billion in SME loans, and serve 150 million Europeans seeking retail banking services. ESBG members are committed to further unleash the promise of sustainable, responsible 21st century banking.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
info@wsbi-esbg.org ▪ www.wsbi-esbg.org

Published by ESBG, June 2018