EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
Do Studzienki Str. 63
80-227 Gdańsk, Poland

tel. +48 58 524 49 01
fax. +48 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Position of the European Financial Congress[1] in relation to the European Commission's consultation document on FinTech: A more competitive and innovative European financial sector[2]

Methodology for preparing the answers

The answers were prepared in the following stages:

Stage 1

A group of experts from the Polish financial sector were invited to participate in the survey. They received selected extracts of the consultation document of the European Commission as well as consultation questions selected by the European Financial Congress. The experts were guaranteed anonymity.

Stage 2

The survey project coordinators from the European Financial Congress prepared a draft synthesis of opinions submitted by the experts. Responses were obtained from experts representing:

- universal banks,
- FinTech companies,
- financial market infrastructure institutions,
- consulting firms.

The draft was sent to the experts participating in the survey with the request to mark the passages that should be modified in the final position and to propose modifications and additions as well as marking the passages they did not agree with and would like them to be removed.

Stage 3

On the basis of the responses received, the final version of the European Financial Congress' answers was prepared.

[1] European Financial Congress (EFC – www.efcongress.com). The purpose of the EFC is to promote debate on how to ensure the financial security and sustainable development of the European Union and Poland.

[2] https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf

Answers of the European Financial Congress to consultation questions[3]

1.2. ***Is there evidence that automated financial advice reaches more consumers, firms, investors in the different areas of financial services (investment services, insurance, etc.) and at what pace? Are these services better adapted to user needs?***

There are several reasons why robo-advice services reach a growing number of customers:

- Few people can afford a specialised investment advisor and the robo-advisors mean much lower fees for management of the customers' assets,
- The Millennials generation uses financial services through their smartphones and put far more trust in technology than their parents do,
- In the future, perfectly polished algorithms will most likely offer faster and more efficient response to market changes than any human being.

Beyond the technological area, automated financial advice is one of the most frequently and willingly developed areas by the FinTech market. It has directly become a part of needs of contemporary customers of advisory services, in particular financial/insurance services. A good example of such services are automated advice services in the ecosystems that support economic activities supplied by banks, advisory firms and suppliers of economic activity management systems. The analysis of entrepreneur behaviour, cash flow or real time accounting allow an immediate response to the needs and problems of the entrepreneur. The Polish market has already seen such solutions and we should expect their further rapid and dynamic growth. The development of such services in the consumer area has been less rapid due to regulatory limitations as regards personal data protection. However, the opportunities offered by new regulations (such as the PSD2) may quickly accelerate the growth rate of advisory services in this area. Market monitoring has shown that automated service mechanisms have reached a wider group of entities, also companies in the financial sector – the automation is moving forward, still there are no hard statistical data on the effects of the changes. It is worth stressing that just like online self-service channels revolutionised the market of banking services and paved the way for cheaper or even free basic services offered to customers, the future robo-advisory automated mechanisms may let the providers offer new services to less affluent customers, for whom the service offered by specialised employees of banks or other financial institutions will be too expensive or such products were too expensive for many segments due to the high cost mark-up.

[3] The questions were selected from a broader pool of questions provided in the European Commission's consultation document. The original numbering has been preserved.

1.4. ***What minimum characteristics and amount of information about the service user and the product portfolio (if any) should be included in algorithms used by the service providers (e.g. as regards risk profile)?***

Algorithms should primarily take into account detailed information about the investor, i.e.:

- Willingness to take risk
- Expected rate of return on the investment
- Age
- Education
- Industry in which they work
- Determination whether the investor accepts for example new technology assets, such as bitcoin, or "unethical" companies, i.e. companies from the tobacco or arms industry

and the investment and selected market:

- Time investment horizon
- Minimum number of assets in the portfolio
- Liquidity of the market on which transactions are concluded
- Nominal value of the portfolio created
- The liquidity reserve required by the investor (to determine what per cent of the investment can be made of non-liquid assets)

Based on this, the algorithm should create the risk profile for the user. Individual customers should be particularly protected against exposure to market risk and informed of all possible scenarios for the investment.

The service provider should be able to identify the person, and the product information should be customised to the buyer. The minimum scope of information should include the amounts that the products apply to, period, product type, fair assessment of possible effects and risk assessment, as well as identification of the pessimistic scenario which the product may trigger (e.g. loss of all funds invested). The risk management policy should be the service provider's responsibility and should be developed along with the development of services and their scale.

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?***

The European Commission may play a major role in the development of FinTech through actions such as:

- Legislative initiatives regulating this market area (e.g. in terms of market and counterparty risk, frauds or transfer of personal data) and also providing friendly framework for the companies to operate in this area

- Support for sandbox projects (regulatory sandboxes) in the Member States to facilitate development of tech start-ups
- Propagation of the information policy with regard to alternative financing mechanisms
- Popularisation of programmes that promote the industry development (e.g. accelerators, hackatons, research projects)
- Cooperation with regional associations of the FinTech ecosystem
- Support for projects aimed at improving scoring models based on which peer-to-peer loans are granted (to date the social data is still an insufficient source that can be easily manipulated)

Considering the goal of crowdfunding campaigns, it should be noted that such goals can be achieved using enhanced investment instruments that are present on the traditional market. To this end, support is required for regulations that promote:

- electronic registration of economic activities based on trust services compliant with standards implemented under the eIDAS Directive – a good example is the S24 procedure used in Poland, which supports registration of economic activities in the form of a limited liability company (*spółka z ograniczoną odpowiedzialnością*), limited partnership (*spółka komandytowa*) and limited joint-stock partnership (*spółka komandytowo-akcyjna*) (work is underway to expand this procedure to allow registration of joint-stock companies (*spółka akcyjna*))
- full dematerialisation of financial instruments (in particular those issued by non-public companies) to enable a fully automated (primary and secondary) trading in such instruments and ensuring that rights in such instruments are exercised (both property and corporate rights) in a way currently available mainly for public securities.
- uniform and consistent application of provisions on public offering, including with regard to instruments distributed through crowdfunding platforms.

The Commission should support a general rule of "single activity – single regulations – single supervision" regardless of the technological solutions used for such activity.

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****?*

Considering the nature of activities of such institutions, efforts should be primarily made to ensure the necessary security of parties to the transactions. The regulatory level should not discriminate any participant of the financing market. Rules, standards and legislation should be at a similar level. A good solution could be regulations allowing/requiring the exchange of information on the parties to the transaction and its subject, as those applicable on the market of traditional bank financing. Regulators should consult their regulatory actions with the community affected by the regulations, since these entities know best what the user of crowdfunding platforms is exposed to. If such companies are willing to develop and gain

greater trust of society, they must provide safe and transparent rules of fund raising. To this end, it is necessary to reach the transparency level ensuring that users trust the funds are used for the described purpose and that there are no instances where an unknown site impersonates a crowdfunding platform raising funds for a noble cause. Such platforms should be subject to key regulations that guarantee security and transparency to customers using such solutions. For example, personal data should be protected, customers should be aware of the risk involved in the transactions they conclude, and the data transparency should prevent abuse.

2.3. ***What kind of impact on employment do you expect as a result of implementing FinTech solutions? What skills are required to accompany such change?***

The required competencies will change. New solutions will eliminate the so-called simple work. Changes will affect back-office, there will be less documentary work. Competencies related to proper understanding how the new solutions work will be required. For analysts, the main task will change. Data collection and alignment will not be necessary. Proper interpretation of the results and analyses received will be crucial. This means demand for much more competent personnel. As regards quantitative issues – a fall in employment should be expected, but due to specific competition requirements, personnel costs should not be expected to decrease.

Development of technologies in the financial market will certainly affect the change in the structure of that employment sector. The traditional banking model based on a network of bank branches gives way to the rising electronic and mobile banking. At the time when new solutions, such as video-verification, document scanning or biometry, allow customers to open accounts or take loans exclusively online, and virtual assistants serve customers better and better, the demand for employment in the areas of direct sales or customer service is falling. In addition, if the Distributed Ledger Technology (DLT) becomes standard, the need for employees of cross-border payments will decline. However, the demand for IT, new technology and compliance staff will grow, as a result of the requirement to implement new international regulations.

Cooperation with start-ups is an opportunity for development of new competencies – smart solutions, creativity, entrepreneurship, shortened time to develop new products. On the other hand, this requires new competencies from us, and a combination of various competencies, which in particular means:

- greater demand for staff who are able to build business solutions based on technology,
- greater demand for IT specialists who are able to work on solutions oriented towards customer needs,
- demand for IT specialists who know new technologies, such as blockchain,
- demand for data science specialists,
- greater use of personnel's potential and skills in the area of customer assistance rather than sales.

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

Cloud services are available for use in the existing legal and regulatory environment, although this requires certain changes and additional actions. As regards cloud computing by financial institutions, regulators are particularly concerned about security of confidential data processing and the ICT environment of the bank, as well as the excessive level of concentration of suppliers of cloud solutions. The Polish regulator issued a recommendation which provides that when the confidential data are processed outside the infrastructure of the bank the bank should:

- establish appropriate controls to ensure the confidentiality of such data (e.g. by encrypting the data);
- ensure that the information about any incidents that threaten data security be reported by the supplier,
- have information on the geographical locations as to where the data are processed and what legal provisions are in force in this regard, and ensure compliance of the provided services with legal regulations in force in Poland,
- ensure effective mechanisms for the secure termination of cooperation (in particular with regard to the return and removal of data – with all copies – by the service provider);
- analyse reasonability, and on these grounds make an appropriate decision concerning the obligation of the supplier to present certificates for compliance with internationally recognised standards of information security (in particular if the data is processed outside the European Economic Area),
- monitor the quality of service and the possibility to control (audit) activities of the third party service provider as regards the services provided to the bank and set clear rules for the exchange and protection of confidential information.

These requirements can be met, but in practice they require detailed arrangements and extensive interactions with the regulator, which prolongs the process. Each cloud solution is examined separately upon request of the bank.

2.6.1. ***Do commercially available cloud solutions meet the minimum requirements that financial service providers need to comply with?***

Commercially available cloud solutions comply with minimum requirements to be met by financial institutions. First, services that are not key services from the viewpoint of stability and continuity of operations of the bank should be addressed, and when experience is gathered, the scope of possible solutions should be expanded during further steps. World leaders who provide cloud solutions guarantee high level of security of the data being processed (strong security teams, high security standards, data replication among Data Centres, ISO 27001 certification, data encryption, strong physical security of the Data Centres). For cloud computing,

when tasks performed for the bank are subject to high security standards met by service providers who undergo audits and meet the requirements of ISO 27001 standard among others, the level of data security will increase and even more advanced security tools will be applied compared to the specialised IT services provided locally. The level of risk related to the use of cloud services for operational work of the bank is acceptable. It should be also stressed that with proper adaptation of the bank's infrastructure, it will be possible to ensure integration with the bank's existing security systems required by the PFSA, such as limitation of access to banking data solely to business computers, control of e-mails sent via the DLP system (data leak monitoring). There are no major technological problems with preparing integration with technological standards used by the banks. Problems and obstacles with potential use of cloud solutions appear when an attempt is made to apply such solutions in the areas (data, products, services) regulated by acts of law or recommendations (national or EU). Given the current regulations, each case of use must be reviewed on an individual basis, considering all the risks and aspects of processes where the cloud would apply (in particular in the context of data to be stored in the cloud). It often happens that even the encryption of data sent and processed in the cloud is not sufficient to meet regulatory requirements or limits the benefits/possibilities that the use of such solutions could offer in place of the IT infrastructure existing within the organisation.

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

A cloud services contract must include specific provisions that guarantee compliance with provisions regarding the management of IT areas and the security of the ICT environment in the banks. Companies in the financial sector should contractually ensure the same conditions as the conditions imposed on them by regulators and meet such SLA as are required in connection with their business. Conditions should be agreed between the entities and the detailed provisions could easily lead to over-regulation, by imposing unreasonable costs on the entities in the financial sector.

Provisions governing confidentiality of the data stored in such cloud solutions are an obvious issue. As additional provisions/guaranties that could be also offered in such commercial clouds, we would recommend an option to select location of servers where the data of the bank (institution from the financial sector) could be stored (option to choose specific servers, countries in which the servers may be located or regions/continents to be excluded from the list of acceptable locations of potential servers). Provision of such obligations could lead to further arrangements that would guarantee full control or monitoring over the data entrusted by the institutions.

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

There is still a number of technological challenges. The most important one is to develop a commercially acceptable algorithm for reaching the consensus. It does not seem that the classic proof-of-work could have more extensive commercial application, and work on the proof-of-stake is progressing much slower than expected. The issue of scalability and efficiency of this class of solutions is also worth stressing. Experience in this scope is still very small. The greatest challenge at the current stage of DLT development seems to be development of a standard for its use and reaching an agreement on common regulations at the international level. In the area of the technology, it will be challenging to develop the infrastructure, and then deal with issues of efficiency and capacity of that system. Much more extensive cooperation between the banks, tech companies and regulators is required. Currently, banks are cautious of DLT technologies and become involved only in the consortia established to test such solutions (e.g. Ripple, R3, Linux). The Distributed Ledger Technology (DLT) is just a technology and as much as a technology. The key challenge is to find a business model where that technology would prove to be considerably cheaper or would bring sufficient benefits, including security and effectiveness (new applications bringing additional value), which would justify investments in this technology.

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?***

Undoubtedly, the greatest obstacles to development of DLT result from the fact that the technologies are developing in an uncertain legal environment. Joint (transnational) regulations are required to establish standards allowing to join various distributed systems (e.g. cross-border cooperation of national systems based on DLT). One of the most important issues in this area is to ensure standardisation of digital identity and smart contracts. Although we have seen the first attempts at standardisation (Chain Open Standard 1), still we need wider cooperation of banks, FinTech and regulators. RODO type regulations could also pose an obstacle to development of such technologies. New technologies (including DLT) work in the area of the same regulations in which traditional solutions operate. Problems with interpretation of regulations may result from the lack of direct references to the technological sphere and the ability to process various types of information and performing of specific activities (e.g. with regard to outsourcing of bank activities, personal data processing). The main legal obstacle to DLT implementation is the lack of regulations that would support unrestricted operation of entities in this area. The European Commission is at the stage of “demystification” of this subject, i.e. the initiation of projects aimed at increasing knowledge among members of EU institutions.

Since the DLT may involve transfers of information that include personal data, requirements of the Act regarding personal data processing will have to be met. The issue that needs consideration is providing a natural person with the right to change and modify the data and

have the data processing stopped. This could be difficult to achieve, since, as a rule, DLT does not provide for deletion or modification of data. It would be also problematic to identify the data controller, and this also will not comply with the current wording of the said Act. Therefore, efficient DLT operation requires legislative changes, among others in the area of personal data protection.

2.11. ***Are the existing outsourcing requirements in financial services legislation sufficient? Who is responsible for the activity of external providers and how are they supervised? Please specify, in which areas further action is needed and what such action should be.***

Regulations of the Polish banking law concerning bank outsourcing and of the Act on Trading in Financial Instruments concerning investment outsourcing require that bank and investment outsourcing be rather strictly supervised by the Polish regulator, the Polish Financial Supervision Authority. Compared to European regulations on bank and investment outsourcing, Polish regulations are more restrictive, which results from the obvious approach under which the supervision extends to actions which are part of activities of a financial institution, regardless of who and where performs such actions. Legal requirements applicable to the use of outsourcing considerably affect decisions made by financial institutions on the use of external providers, and the institutions often avoid this type of cooperation due to security requirements. In general, the Polish law does not regulate outsourcing, beyond some sectoral exceptions. Such an exception is bank outsourcing, the use and conditions of which are limited under statutory provisions. The scope of actions that may be the subject of outsourcing is governed in the said Act on a case-law basis. The requirements and method of contract performance is regulated in detail. The most important issue is joint liability of the bank and the IT provider for damage caused to customers as a result of non-performance or improper performance of the outsourcing agreement – this liability cannot be excluded or limited. In Poland, requirements applicable to outsourcing are restrictive. It does not seem advisable to introduce additional regulations in the field of outsourcing, unless the goals of such regulations would be to harmonize requirements for the entire European Union.

3.4. ***Should the EU introduce new licensing categories for FinTech activities with harmonised and proportionate regulatory and supervisory requirements, including passporting of such activities across the EU Single Market? If yes, please specify in which specific areas you think this should happen and what role the ESAs should play in this. For instance, should the ESAs play a role in pan-EU registration and supervision of FinTech firms?***

FinTechs can operate under market rules in the same way as other economic activities or other companies. Introduction of new forms of licensing and industry categories would give rise to bureaucracy and formalism, which often presents a barrier to development of innovations. All market participants should be treated equally. Removing barriers to enter the market and facilitating operation of financial start-ups should be introduced very carefully, due to the high risk for the entire sector. As the consultation document rightly mentions, the same type of

activities should be subject to the same type of rules. The fact that modern technological solutions can be applied for certain types of activities may not legitimize allowances for them. What is more, the modern technology requires a more careful approach, in particular at the early stages of its application.

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

Neutrality, proportionality and integrity are universal principles, applicable not only to FinTech operations. Certainly, they are right, but they are not the only principles. The discussion applies to the use of technological solutions in financial institutions. New technologies may function on the market on their own, as independent enterprises, which perform certain activities for the financial institutions. They may enter an organisation and be part of it. If we are dealing with an independent entity, it is necessary to invoke the fourth principle: new solutions must not compromise in any way the security of an institution and funds held by the institution. Outsourcers approach this principle with reluctance. However, the failure to meet this principle may put security of the financial system at risk, even on a major scale, due to operational risk and the contagious effect.

3.8. ***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?***

The European Commission and ESA should support creation of innovation hubs, accelerators and regulatory sandboxes. We expect that the role of such solutions will be to support innovative ventures and provide assistance in achieving compliance with regulatory requirements. First, such solutions should be launched at the level of individual Member States, since this is where supervision over the financial market is maintained.

Local practices of this kind may potentially encounter limitations where the projects face issues related to community regulations directly applied (Regulations of the European Commission). In addition, projects have an increasingly cross-border dimension and support from the local regulator only may prove to be insufficient. Finally, some projects are based on the technological integration with the transnational infrastructure, such as the common currency (euro - also in the expected virtual form), Target2, T2S or SEPA clearing systems. In such situations, to ensure efficient operations of local solutions, it is necessary to establish an adequate partner centre at the EU level that would provide support on community regulations, as well as coordination and harmonization of initiatives, such as:

- support for sandbox projects (regulatory sandboxes) in the Member States to facilitate development of tech start-ups,

- popularisation of programmes that promote industry development (e.g. accelerators, hackatons, research projects),
- cooperation with regional associations of the FinTech ecosystem,
- creation of co-working places in public space,
- EU fund programmes to promote development of new technologies.

3.12.1. ***Is the development of technical standards and interoperability for FinTech in the EU sufficiently addressed as part of the European System of Financial Supervision?***

The specific nature and strength of FinTech is the lack of or limited regulations, which give way to innovations, often customised to individual markets. There is no need for regulations that would require interoperability. What is more, at the current stage of Internet development and API approach, it could be assumed that interoperability, if backed by business rationale, will appear without any regulatory initiatives.

3.12.2. ***Is the current level of data standardisation and interoperability an obstacle to taking full advantage of outsourcing opportunities?***

Standardisation and interoperability is not an obstacle to outsourcing. The diversity of solutions is the genesis of innovation and the full standardisation of processes would not be beneficial to the market. The standardisation in selected key areas is adequate (a good example are SEPA – SCT transfers or eIDAS).

3.13. ***In which areas could EU or global level standards facilitate the efficiency and interoperability of FinTech solutions? What would be the most effective and competition-friendly approach to develop these standards?***

The EU standards should first of all standardize the law in the area of new financial technologies and make it transparent and comprehensible to new companies entering that market. Surely sandbox projects increase the effectiveness and facilitate deployment of new FinTech solutions. Development of standard API messages within e.g. ISO 20022 etc. could contribute to the development. It should be remembered that development cycles of standards, e.g. ISO, are not sufficiently fast and the market should not be limited to use the existing standards only, since this would hamper innovations, which as a rule need the room to go beyond existing standards.

4.2. ***To what extent could DLT solutions provide a reliable tool for financial information storing and sharing? Are there alternative technological solutions?***

Although the scale of technology use cannot be compared to traditional technologies, experience in the market of virtual currencies (Bitcoin) demonstrates that DLT solutions are

secure, reliable and can be commonly applied as an alternative to existing solutions. In our opinion, it is only a matter of time until the technology is used in a wider context, which will generate high savings related to storage and protection of data (no middlemen, reduction in the costs of security and maintenance). DLT supports development of decentralised networks to store and manage data, where a central site is no longer required. In addition, information stored in the DLT is, by definition, resistant to attempts at unauthorized tampering, so the data that are correctly input into the DLT remain unchanged. It is a distinguishing feature of the DLT, which makes it an adequate tool to store proofs of ownership or existence. There is a number of financial processes and services that may benefit from this unchanging storage. Information about customers, information about contracts, ownership rights, cryptographic keys replacing traditional signatures are only some of the types of information that could be stored in the DLT.

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?***

The key barriers include:

- limitations in personal data protection upon access, informing, prevention or investigations related to crime detection or fraud prevention,
- various regulations of individual countries – different legal classification of individual offences or misdemeanours,
- lack of ability to rapidly respond to cybercrime involving several countries (no real-time cooperation of the police, no 'internet police').

The diversity of solutions used by entities from the financial sector is a part of security of such services. Full standardisation would imply greater system risk in the event of a security breach. The diversity that is beneficial for the financial sector and the risk-based approach results in the lack of full interoperability of systems, which is a natural, albeit secondary barrier to information exchange. Main barriers is the natural protection of own data against competitors and regulatory limitations with regard to personal data or banking secrecy, which means that not all potentially data valuable for counteracting cybercrime can be shared. To share knowledge of cyberthreats, sectoral cooperation (e.g. among banks, providers of telecommunication infrastructure, within the public sector) and inter-sectoral cooperation is necessary to facilitate identification of threats. In Poland, there are basically no such barriers. For years, financial institutions have cooperated with each other and state institutions, police and other dedicated institutions and have exchanged information through a dedicated platform. In 2016 the Cyber Security Centre was established, where banks, telecoms and representatives of governmental institution develop effective forms of cooperation, communication and information exchange.